

**ESCUELA TÉCNICA SUPERIOR DE INGENIEROS  
INDUSTRIALES Y DE TELECOMUNICACIÓN**

**UNIVERSIDAD DE CANTABRIA**



***Proyecto Fin de Carrera***

**DESPLIGUE DE UNA CELDA GSM BASADA  
EN SISTEMAS ABIERTOS**

**Deploying a GSM cell based on open systems**

Para acceder al Título de

**INGENIERO DE TELECOMUNICACIÓN**

**Autor: Arturo Rivas Arias**

**Octubre – 2013**

# **INGENIERÍA DE TELECOMUNICACIÓN**

CALIFICACIÓN DEL PROYECTO FIN DE CARRERA

**Realizado por: Arturo Rivas Arias**

**Director del PFC: Jorge Lanza Calderón**

**Título: “Despliegue de una celda GSM basada en sistemas abiertos”**

**Title: “Deploying a GSM cell based on open systems”**

**Presentado a examen el día: 31 de Octubre de 2013**

para acceder al Título de

**INGENIERO DE TELECOMUNICACIÓN**

Composición del Tribunal:

Presidente (Apellidos, Nombre): Luis Sánchez González

Secretario (Apellidos, Nombre): Jorge Lanza Calderón

Vocal (Apellidos, Nombre): Roberto Sanz Gil

Este Tribunal ha resuelto otorgar la calificación de:

.....

Fdo.: El Presidente

Fdo.: El Secretario

Fdo.: El Vocal

Fdo.: El Director del PFC  
(sólo si es distinto del Secretario)

Vº Bº del Subdirector

Proyecto Fin de Carrera Nº  
(a asignar por Secretaría)

# Agradecimientos

---

Quiero aprovechar estas líneas para agradecer a todas las personas que de alguna u otra forma me han apoyado en mi andadura por lo que considero la gran vocación de mi vida, el mundo de las telecomunicaciones.

En primer lugar a quería agradecer el apoyo a mi familia y a la que considero una más de ella, mi novia. A mi novia Leticia por su paciencia y por mostrarme los mejor de mí y de lo que soy capaz sin dejar ni un solo momento de hacerme sentir tan especial. A mi madre por apoyarme en todo momento y por darme todo sin pedir nada a cambio. A mi hermano Javier por abrir el camino en este mundo de la tecnología y no dejar que me rudiese nunca. A mi padre Javier que sé que me estará viendo desde algún sitio y que nada me hace más feliz que darle motivos para que se sienta orgulloso de mi. También a mis abuelos, tíos y primos que por la distancia veo poco pero que siempre tenían un “que no te queda nada” para ofrecer apoyo.

Por supuesto no me olvido de mis compañeros de la carrera con los que he coincidido en alguna asignatura o evento, que aunque son muchos y no puedo nombrarles, siempre han ofrecido su apoyo a la hora de estudiar o desconectar después de algún día nefasto.

A los amigos que he conocido en León, Felechas y Santander porque en ocasiones ha sido complicado compaginar trabajo y proyecto pero siempre estaban ellos para animarme, aunque a veces me diesen caña pero de la que también se agradece.

A todos los profesores con los que he coincidido durante la carrera que, por interés u obligación por mi parte, han puesto todo su empeño en que cada día fuese un poco menos ignorante que el anterior. En especial a Jorge por su ayuda y perseverancia debido al poco tiempo que yo tenía disponible. Ha sido un placer haber aprendido de él.

# Resumen

---

Las redes de comunicaciones inalámbricas suponen en la actualidad uno de los negocios más importantes a lo largo del planeta. Además son un claro ejemplo de empuje tecnológico gracias a la amplia demanda por parte de los clientes. Esto impulsa a operadores y fabricantes de equipamiento a evolucionar sus productos de forma continua a la vez que crean nuevas necesidades en los clientes que desean contar siempre con el producto más avanzado. Pero la industria de las telecomunicaciones móviles siempre se ha caracterizado por su carácter cerrado. Tanto los equipos como el acceso a la configuración de red está reservada únicamente a los operadores. A pesar de que en la actualidad han surgido pequeñas empresas que realquilan partes de la red a los operadores establecidos, el altísimo precio por la concesión de licencias de espectro radioeléctrico imposibilita una competencia abierta y libre entre los interesados. Debido a ello, es muy difícil lograr un acceso a la red para lograr entornos de pruebas o para ofrecer servicios sobre las mismas. Surge entonces la necesidad de buscar alternativas que permitan analizar redes, ya sea con fines estadísticos o educativos, o realizar implementaciones de pequeñas estaciones base para pruebas, cubrir zonas de baja demanda o con fines pedagógicos proporcionando una red libre y que pueda configurarse, operarse y mantenerse bajo el control total del usuario. La manera de proceder será encontrar equipos radiantes con un coste moderado y que sean compatibles con un software capaz de controlarlos. Para ello se recurre al software libre, que además de no suponer coste su utilización, cuenta con multitud de opciones para completar su desarrollo en los apartados que resulten más interesantes para el usuario. Utilizando una implementación de este tipo, podemos realizar algunos procedimientos que ponen en duda la seguridad de los estándares de comunicaciones y que permiten capturar la información que circula por la red. Es una muestra de que la tecnología no está exenta de fallos y aunque los desarrollos mejoren con cada nueva versión, siempre habrá algún agujero de seguridad que resulte imposible de ocultar.

# Abstract

---

Wireless telecommunication networks are one of the most important businesses all over the world nowadays. In addition to that, they are a clear example of a technology that is pushed to its limits due to the big demand by the costumers. This demand encourages services providers and equipment manufacturers to develop their products on an ongoing basis and creates new needs from clients who want to have the most advanced product. However the mobile industry has always been characterised by its closed nature. Both equipment and access to the network settings are reserved only operators. Despite of that, in the last few years, some small companies have emerged and they are trying to sub-let pieces of the network from the big services providers, however the high price for the licensing of the radio spectrum precludes open and free competition among concerned. Because of that, it is very difficult to gain access to a network to perform any kind of testing or to provide your own service over it. This brings the need to seek alternative options to analyse networks, both for statistical or educational purposes, or small deployments of base stations for testing, covering areas of low demand or for educational purposes and to provide a free network that can be configured, operated and managed under the control of the user. The way forward is to find transmission systems at a moderate cost and compatible with software that will be able to control them. Here is where we turn to free software, because as well as not incurring in any cost for using it ,offers the possibility of developing it further in the areas that are most interesting to the user. Using such an implementation, we can perform some steps which compromise the security of the communication standards and allow to catch the information that is moving through the network. It is proof that technology is not free of issues and although every new version brings in new improvements in software and hardware, there will always be a security hole that is impossible to hide.

# Índice

---

<b>1</b>	<b>INTRODUCCIÓN Y OBJETIVOS</b>	<b>2</b>
1.1	COMUNICACIONES MÓVILES	2
1.2	OBJETIVO DEL PROYECTO FIN DE CARRERA	3
<b>2</b>	<b>ESTÁNDAR DE TELECOMUNICACIONES GSM</b>	<b>7</b>
2.1	PRIMERAS REDES DE COMUNICACIONES	7
2.2	REDES GSM	8
2.2.1	INTERFAZ RADIO	9
2.2.1.1	Características físicas	10
2.2.1.2	Canales lógicos de control	12
2.2.1.3	Canales lógicos de tráfico	13
2.2.1.4	Formato ráfagas GSM	14
2.2.2	RED TRONCAL	15
2.2.3	ARQUITECTURA DE LAS REDES GSM	15
2.2.3.1	Estación móvil	16
2.2.3.2	Subsistema de estación base	16
2.2.3.3	Subsistema de red y conmutación	18
2.2.3.4	Subsistema de operación y mantenimiento	19
2.3	GPRS	20
2.3.1	ARQUITECTURA GPRS	20
2.3.2	ENRUTADO DE LOS PAQUETES	22
2.4	IMPLEMENTACIÓN DE SISTEMAS GSM	22
2.4.1	IMPLEMENTACIÓN DE ESTACIONES BASE GSM	22
2.4.2	IMPLEMENTACIÓN DE ANALIZADORES DE REDES MÓVILES	24
<b>3</b>	<b>ESTADO DEL ARTE EN REDES MÓVILES</b>	<b>28</b>
3.1	DESPLIEGUE DE REDES MÓVILES EN ESPAÑA	28
3.1.1	SUBASTA DE BLOQUE DENTRO DE LAS BANDAS DE FRECUENCIA	28
3.1.2	OPERADORAS MÓVILES VIRTUALES (OMV)	29
3.2	LEGISLACIÓN DEL ESPECTRO RADIOELÉCTRICO EN ESPAÑA	30
3.3	NUEVA GENERACIÓN DE COMUNICACIONES: LTE	31
<b>4</b>	<b>ANALIZADOR DE REDES GSM</b>	<b>34</b>
4.1	PROYECTO OSMOCOMBB	34
4.2	SOFTWARE PARA EL TERMINAL MÓVIL	35
4.3	SOFTWARE PARA EL PC	36
4.4	INTEGRACIÓN CON ANALIZADOR DE PROTOCOLOS (GSMTAP)	37
4.5	MANEJO Y OBTENCIÓN DE RESULTADOS	39
4.5.1	ARRANQUE DEL ANALIZADOR	39
4.5.2	OBTENER INFORMACIÓN MEDIANTE TERMINAL	40
4.5.2.1	Información acerca de la estación móvil	40
4.5.2.2	Información sobre celdas GSM	42
4.5.3	OPERACIONES SIM MEDIANTE TERMINAL	45
4.5.4	ANÁLISIS CON WIRESHARK	45
4.5.4.1	Análisis de canales lógicos de control	46
4.5.4.2	Estudio de procedimientos realizados por el terminal dentro de la red	49
4.5.4.2.1	Primer acceso a la red	49
4.5.4.2.2	Realización de llamadas de voz	51
4.5.4.2.3	Envío y recepción de SMS	56

<b>4.6 OPCIONES Y VENTAJAS DEL PROYECTO OSMOCOMBB .....</b>	<b>58</b>
<b><u>5 DESPLIEGUE DE UNA CELDA GSM.....</u></b>	<b><u>62</u></b>
<b>5.1 OPENBSC DE OSMOCOM .....</b>	<b>62</b>
<b>5.2 IMPLANTACIÓN DE UN SISTEMA GSM DE BAJO COSTE Y SOFTWARE LIBRE .....</b>	<b>63</b>
5.2.1 NANOBTB .....	63
5.2.2 OSMO-NITB .....	65
5.2.2.1 Implementación del HLR .....	66
5.2.3 USO Y OPERACIÓN DE NUESTRA ESTACIÓN BASE.....	67
5.2.4 OPERACIONES DISPONIBLES EN NUESTRA ESTACIÓN BASE .....	70
5.2.4.1 Información sobre el estado de la red.....	71
5.2.4.2 Información y operaciones sobre los terminales asociados .....	72
5.2.4.3 Operaciones sobre la estación base.....	73
5.2.5 SERVICIOS DE VOZ Y SMS.....	74
<b><u>6 INTEGRACIÓN DE CELDA GSM CON CENTRALITA VOIP Y LA RTC .....</u></b>	<b><u>76</u></b>
<b>6.1 INTEGRACIÓN CON CENTRALITA DE VOIP .....</b>	<b>76</b>
6.1.1 INSTALACIÓN Y CONFIGURACIÓN DEL SOFTWARE NECESARIO .....	77
6.1.2 CONFIGURACIÓN BÁSICA DE ASTERISK .....	78
6.1.2.1 sip.conf.....	78
6.1.2.2 extensions.conf .....	79
6.1.2.3 routing.conf .....	79
6.1.3 USO Y OPERACIÓN DEL SISTEMA A TRAVÉS DE LA CENTRALITA ASTERISK.....	79
<b>6.2 CONEXIÓN CON LA RTC .....</b>	<b>81</b>
6.2.1 CONFIGURACIÓN DEL ATA SPA-3102.....	82
6.2.2 CONFIGURACIÓN DE LA PBX ASTERISK .....	84
6.2.2.1 Extensión SIP equivalente al ATA .....	85
6.2.2.2 Nuevo contexto para llamadas entrantes y adicción para llamada salientes..	85
6.2.3 USO Y OPERACIÓN DEL SISTEMA PARA COMUNICACIÓN CON LA RTC .....	86
<b>6.3 OPCIONES Y VENTAJAS DEL PROYECTO OPENBSC .....</b>	<b>87</b>
<b>6.4 SEGURIDAD DEL ESTÁNDAR GSM .....</b>	<b>89</b>
6.4.1 FALTA DE AUTENTICACIÓN MUTUA.....	89
6.4.2 ATAQUE A LAS COMUNICACIONES DE VOZ GSM MEDIANTE ESTACIÓN BASE FALSA..	89
6.4.3 EXTENSIÓN DEL ATAQUE A OTRAS REDES DE COMUNICACIONES.....	90
<b><u>7 CONCLUSIONES Y LÍNEAS FUTURAS .....</u></b>	<b><u>92</u></b>
<b>7.1 ANALIZADOR DE REDES GSM .....</b>	<b>92</b>
7.1.1 IMPLICACIONES DEL ANALIZADOR DE REDES.....	92
7.1.2 LÍNEAS FUTURAS DEL ANALIZADOR DE REDES .....	93
<b>7.2 ESTACIÓN BASE GSM .....</b>	<b>94</b>
7.2.1 IMPLICACIONES DE LA ESTACIÓN BASE.....	94
7.2.2 PRÓXIMOS OBJETIVOS DEL PROYECTO OPENBSC .....	95
7.2.3 PROYECTO OPENBSC_GPRS .....	95
<b><u>8 BIBLIOGRAFÍA .....</u></b>	<b><u>97</u></b>
<b><u>9 ACRÓNIMOS.....</u></b>	<b><u>101</u></b>
<b><u>10 APÉNDICES.....</u></b>	<b><u>106</u></b>
[APÉNDICE1] OPENBSC.CFG .....	106
[APÉNDICE2] SIP.CONF .....	109
[APÉNDICE3] EXTENSIONS.CONF .....	110
[APÉNDICE4] ROUTING.CONF .....	111



# Índice de Tablas

---

Tabla 1: Datos contenidos en la tarjeta SIM.....	9
Tabla 2: Bandas de frecuencias fijadas por el estándar GSM .....	10
Tabla 3: Comparativa de equipos analizadores de redes Wi-Fi .....	24
Tabla 4: Elementos cabecera GSMTAP.....	38
Tabla 5: Correspondencia ARFCN con frecuencia principal.....	42
Tabla 6: Modelos y precios de los equipos utilizados.....	59
Tabla 7: Parámetros en la base de datos de abonados .....	66
Tabla 8: Direcciones de red de los equipos .....	67
Tabla 9: Parámetros clave de configuración del software osmo-nitb.....	68
Tabla 10: Distribución de canales en la nanoBTS.....	68
Tabla 11: Datos de abonados en el HLR .....	74
Tabla 12: Configuración de línea PSTN (RTC) en el SP3102 .....	84
Tabla 13: Modelos y precio de los componentes del sistema.....	87

# Índice de imágenes

---

Ilustración 1: Estación base de telefonía móvil.....	4
Ilustración 2: Distribución de canales en el estándar GSM .....	11
Ilustración 3: División y decalado temporal en GSM .....	11
Ilustración 4: Slot 0 de la frecuencia central: canal descendente (arriba) y canal descendente (abajo) .....	12
Ilustración 5: Distribución de canales TCH/F + SACCH .....	13
Ilustración 6: Distribución de canales TCH/H + SACCH.....	13
Ilustración 7: Ráfaga normal del estándar GSM.....	14
Ilustración 8: Ráfaga de acceso del estándar GSM .....	14
Ilustración 9: Ráfaga S del estándar GSM .....	14
Ilustración 10: Arquitectura de red GSM .....	15
Ilustración 11: Subsistema de estación base .....	17
Ilustración 12: Interconexión del BSS con el NSS.....	17
Ilustración 13: Subsistema de red y conmutación .....	18
Ilustración 14: Subsistema de operación y mantenimiento.....	19
Ilustración 15: Arquitectura de redes GSM con servicio GPRS .....	21
Ilustración 16: Ejemplos de analizadores comerciales .....	25
Ilustración 17: LTE Smart Analyzer de RADCOM .....	25
Ilustración 18: Analizador GSM K15 de Tektronics .....	25
Ilustración 19: Mapa de bandas de frecuencia de telefonía en España.....	29
Ilustración 20: Despliegue de tecnología LTE en España por empresa y fecha .....	32
Ilustración 21: Logotipo del proyecto OsmocomBB.....	34
Ilustración 22: Esquema general analizador GSM .....	34
Ilustración 23: Terminales de salida de datos, osmocom a la izquierda y mobile a la derecha.....	36
Ilustración 24: Esquema de funciones dentro de cada elemento .....	37
Ilustración 25: Software de análisis de protocolos WireShark .....	37
Ilustración 26: Conexión del terminal con el PC .....	39
Ilustración 27: Captura de datos con SIM personalizada .....	41
Ilustración 28: Captura de datos con SIM del operador Movistar .....	41
Ilustración 29: Redes disponibles para la SIM personalizada.....	42
Ilustración 30: Redes disponibles para SIM del operador Movistar .....	42
Ilustración 31: Información sobre celdas vecinas.....	43
Ilustración 32: Parámetros de reelección de celda .....	44
Ilustración 33: Canales y operadores de las celdas adyacentes .....	44
Ilustración 34: Encapsulado de trama en WireShark.....	46
Ilustración 35: Cabecera GSMTAP .....	47
Ilustración 36: Trama PAGCH.....	47
Ilustración 37: Campo 'Celdas vecinas' en trama BCCH .....	48
Ilustración 38: Trama BCCH con parámetros e identificación de celda .....	48
Ilustración 39: Captura de asignación inmediata.....	49
Ilustración 40: Diagrama de flujo para acceso a la red.....	50
Ilustración 41: Procedimiento de acceso a la red.....	50
Ilustración 42: Trama 41 con medidas en el interfaz radio .....	50
Ilustración 43: Trama 42 con datos sobre la interfaz móvil.....	51
Ilustración 44: Trama 53 de confirmación del proceso de actualización de posición ...	51
Ilustración 45: Diagrama de flujo de llamada entrante.....	52
Ilustración 46: Tramas iniciales para el establecimiento de llamada saliente .....	52
Ilustración 47: Trama de solicitud de servicio de llamada saliente .....	53
Ilustración 48: Trama de configuración de llamada saliente .....	53
Ilustración 49: Tramas de establecimiento de llamada saliente.....	53

Ilustración 50: Tramas de desconexión de la llamada saliente.....	54
Ilustración 51: Diagrama de flujo llamada entrante .....	54
Ilustración 52: Tramas iniciales de establecimiento de llamada entrante .....	55
Ilustración 53: Tramas de establecimietno de llamada entrante .....	55
Ilustración 54: Tramas de conexión de llamada entrante .....	55
Ilustración 55: Tramas de desconexión de llamada entrante.....	55
Ilustración 56: Petición de servicio SMS .....	56
Ilustración 57: Tramas de datos SMS saliente .....	56
Ilustración 58: Detalle de trama de datos SMS saliente .....	57
Ilustración 59: Tramas de desconexión del servicio SMS .....	57
Ilustración 60: Tramas de información SMS entrante.....	57
Ilustración 61: Detalle trama de datos SMS entrante .....	58
Ilustración 62: Equipos utilizados para el analizador.....	59
Ilustración 63: nanoBTS GSM de ip.access .....	64
Ilustración 64: Equipos necesarios para realizar la implementación.....	64
Ilustración 65: Arquitectura de la estación base basada en OpenBSC.....	65
Ilustración 66: Consolda de salida al inicio de osmo-nitb .....	69
Ilustración 67: Selección manual de red en terminal GSM .....	69
Ilustración 68: Terminal asociado a nuestra estación base .....	70
Ilustración 69: Estado de la red GSM.....	71
Ilustración 70: Información sobre la BTS.....	71
Ilustración 71: información sobre el TRX.....	72
Ilustración 72: Estadísticas referentes a la red.....	72
Ilustración 73: información del abonado con ID 4.....	72
Ilustración 74: Operaciones sobre la base de datos de usuarios .....	73
Ilustración 75: Opciones de configuración de la estación base .....	73
Ilustración 76: Llamada (izquierda) y SMS (derecha) entrantes .....	74
Ilustración 77: Esquema de interconexión de los diferentes elementos .....	76
Ilustración 78: Configuración usuario SIP .....	80
Ilustración 79: Arranque del programa LCR .....	80
Ilustración 80: Arranque osmo-nitb con socket MNCC .....	80
Ilustración 81: Llamada recibida en extensión SIP(izquierda) y móvil(derecha) .....	81
Ilustración 82: Esquema del sistema GSM completo con la salida a la RTC .....	81
Ilustración 83: Montaje de ATA conectado a router.....	82
Ilustración 84: Detalle de los puertos utilizados en el ATA .....	83
Ilustración 85: Panel de configuración SPA 3102.....	83
Ilustración 86: Configuración de red en el ATA .....	83
Ilustración 87: Esquema de conexión ATA.....	86
Ilustración 88: Equipos utilizados para OpenBSC + Asterisk + ATA.....	88

# Capítulo 1 – Introducción y objetivos

# 1 Introducción y objetivos

Si miramos a nuestro alrededor, seguramente encontremos a alguien con un pequeño aparato pegado a su oreja y hablando solo, o mirándolo fijamente mientras parece que dibuja algo sobre él con su dedo índice, o incluso seamos nosotros mismos los que estemos sosteniendo uno de estos aparatos. Y es que la telefonía móvil es sin duda alguna uno de los productos de más rápida adopción por parte de los consumidores. Es el ejemplo perfecto de empuje tecnológico, la amplia demanda del producto creó nuevas necesidades y facilitó que multitud de gobiernos y empresas invirtiesen millones de euros en el desarrollo de tecnologías y terminales de comunicaciones.

Para que exista una comunicación inalámbrica deber existir, al igual que para establecer cualquier tipo de comunicación, un emisor, un receptor y un canal. Vamos a conocer con más detalle las particularidades de las comunicaciones inalámbricas y qué las hace tan importantes.

## 1.1 Comunicaciones Móviles

Aunque parece que llevan entre nosotros algo más de 10 años, las primeras comunicaciones inalámbricas datan de principios de siglo. El ingeniero Guillermo Marconi [1] consiguió en el año 1901 el primer sistema de comunicaciones útil, logró la primera emisión radioeléctrica transatlántica. Aunque el estudio de la radiofrecuencia es necesario para el tema que nos ocupa, existe una diferencia fundamental entre los sistemas de comunicaciones inalámbricos y los sistemas de comunicaciones móviles. Un sistema de comunicaciones inalámbrico es aquel que consigue transmitir información (analógica o digital) de un emisor a un receptor sin necesidad de un medio físico cableado. Naturalmente se emplea un medio físico para la comunicación y en este caso dicho medio utilizado es la atmósfera terrestre, pero lo que hace a estos sistemas realmente útiles es que no necesitan una instalación del canal de comunicaciones para transmitir la información, sólo un equipo emisor y un receptor. La comunicaciones inalámbricas ofrecen la libertad de movimientos dentro del área de cobertura que suponga la correcta recepción de la información el receptor. En este sentido, la gestión inteligente de las tecnologías y canales de comunicación inalámbrica, permite extender el área de movimiento. Así surge el concepto de movilidad soportado por las redes de comunicaciones móviles.

Para conseguir movilidad en las comunicaciones hubo que esperar casi medio siglo y los primeros dispositivos móviles se comenzaron a utilizar durante la segunda guerra mundial. El concepto de movilidad en las comunicaciones implica que emisor y receptor no necesitan estar en una posición fija sino que pueden variar esta durante la comunicación. En la actualidad ni siquiera es necesario que los equipos que realizan la comunicación tengan visión directa sino que la tecnología posibilita que éstos puedan comunicarse siempre y cuando tengan unos mínimos de intensidad de señal y ruido. Aunque esto supone una gran ventaja, las zonas de influencia de los terminales son limitadas. Para ello se pensó en los repetidores. Estos repetidores se colocarían en posiciones fijas dentro de la zona a cubrir por el sistema y el más cercano al emisor captaría la señal, la transmitiría por un red hasta el repetidor más cercano al receptor y este se la enviaría a su destinatario. De esto se deriva el concepto de cobertura o zona en las que los repetidores son capaces de comunicarse con los terminales.

De estos principios se derivan todas las redes y terminales que pueden encontrarse hoy en día. Bien es cierto que ha evolucionado mucho la forma de enviar la

información, de distribución de antenas, la potencia de los terminales... pero todos los sistemas tienen la misma estructura básica: los repetidores, las conexiones entre los mismo y los terminales que emiten y reciben. También ha cambiado la información que se transmite, pasando de voz o pequeños mensajes a localización, contenido multimedia, correo electrónico... Es curioso cómo algo que lleva tan poco tiempo existiendo pueda hacer que millones de consumidores hayan modificado de forma significativa la forma de concertar citas, hablar sobre el partido de su equipo favorito o enseñar las fotos de sus vacaciones. Y no sólo eso, desde que la telefonía móvil se popularizó, hemos cambiado incluso la forma de utilizarla. Si bien hace 7, 8 o incluso 9 años enviábamos algunos SMS, hoy podemos enviar cientos de *WhatsApps* en un solo día.

Aunque hablamos de una tecnología de principio del siglo XX, no ha sido hasta la entrada del XIX cuando la telefonía se ha abierto al público de forma masiva. Ahora mismo nos encontramos ante uno de los negocios más grandes a nivel mundial. Dejando a un lado a las compañías petroleras, las empresas más importantes en la actualidad tienen algo que ver en el negocio de la telefonía móvil. Algo curioso es que no se trata de compañías denominadas operadoras que poseen su red de distribución para dar servicio a lo usuarios sino que las más rentables son las que fabrican los terminales que operan sobre la red y que además prestan servicios de valor añadido sobre la misma.

En España ya contamos con más líneas móviles que habitantes. En el años 2012, la principales agencias [2] de estadísticas indicaban que se habían superado los 6.000 millones de líneas en todo el mundo. Aunque es una cifra enorme, es necesario indicar que no tiene en cuenta si varias líneas pertenecen a un mismo usuario. El problema en cuanto a la red de distribución del servicio móvil, es que se trata de una infraestructura cerrada. Los operadores soportan estos servicios pero no permiten modificar configuraciones, procedimientos o características dentro de la red. Por ello se han buscado soluciones en este proyecto que permitan la creación de una red con algunos de los servicios de las redes móviles comerciales pero basadas en soluciones abiertas que permitan la personalización y configuración de la red. Se trata de un campo que ha cobrado importancia en los últimos años donde las necesidades de ancho de banda y calidad de las comunicaciones están haciendo necesaria la instalación de un mayor número de estaciones base pero de bajo radio de acción.

## 1.2 Objetivo del proyecto fin de carrera

Se ha comentado anteriormente que las actuales redes de los operadores demasiado cerradas y no permiten al usuario avanzado interactuar con las mismas de la forma que desearía. Además todos lo elementos de análisis o simulación basado en los estándares de redes de comunicaciones móviles son demasiado caros. El equipamiento y las licencias software son difícilmente asumibles para entornos de aprendizaje o pruebas.

Debido a la gran expansión y las múltiples utilidades que se derivan de las redes de comunicaciones móviles, se ha propuesto realizar sendas plataformas que no permitan por un lado el análisis de redes capturando el tráfico que circula por ellas y por otra la creación de una pequeña celda de comunicaciones autosuficiente. Al tratarse de montajes aptos para laboratorios y entornos reducidos, el requisito indispensable era ajustar lo más posible el presupuesto llegando a un equilibrio entre las prestaciones que nos ofrece y el coste las mismas.

El primer objetivo del presente proyecto es conseguir un analizador espectral de bajo coste que sea capaz de capturar el tráfico emitido por las antenas y los terminales de comunicaciones. Además, deberá recoger los datos e interpretar las diferentes unidades de información para simplificar el análisis. Será útil también para conocer las peculiaridades del estándar GSM a fin de facilitar la configuración de la implementación de la estación base que se propone en la segunda fase del proyecto.

Una vez estudiado el estándar y conocidos su funcionamiento y estructura, se pretende conseguir una infraestructura de red capaz de dar servicio a terminales compatibles con el estándar móvil de segunda generación. Se deberá conseguir una red abierta desde el punto de vista de configuración en la que se puedan variar los parámetros de emisión de la antena, la potencia... así como la gestión de los abonados que puedan acceder a la misma.



Ilustración 1: Estación base de telefonía móvil

Antes de entrar en la parte más técnica, se describirán los procedimientos y la infraestructura del estándar GSM. Además se mostrará la evolución dentro del territorio nacional de las redes de comunicaciones móviles. Se mostrará entonces el funcionamiento de la implementación del entorno de análisis y operación de redes GSM realizado y se concluirá con algunas consideraciones de seguridad inherentes a dichas redes. El proyecto se estructura en 5 bloques:

### Redes GSM:

Descripción del estándar de segunda generación. Aquí se incluyen todos los protocolos que utiliza la red así como los procedimientos que permiten operar dentro de la red. También se hablará de la infraestructura necesaria para crear una red GSM.

### Estado del arte:

Se comentarán las peculiaridades de la implantación de las primeras redes GSM en España y su evolución temporal. Además se mostrará el reparto de licencias a operadores y la importancia de esta adjudicación para el desarrollo de la tecnología.

### Analizador GSM:

Se dará a conocer la solución aplicada para la creación de un sistema capaz de interpretar los datos característicos de las redes GSM y las posibilidades que permite desarrollar el sistema elegido. Se describirán los equipos y el software utilizado.

### Estación base GSM:

Hablaremos de cómo implementar una red completa que soporte los servicios más importantes dentro de la red. Se mostrarán las diferentes configuraciones y su efecto sobre el sistema así como las diferencias funcionales con las redes comerciales pertenecientes a los operadores.

### Conexión con otros sistemas:

Por último se detallarán los mecanismos que existen para interconectar nuestra red GSM con otros sistemas que actuarán como centralita y permitirán mayor margen a la hora de configurar el direccionamiento de las llamadas. Además conectaremos nuestra estación base a la red pública para poder realizar una comunicación con cualquier teléfono de un operador convencional. Al poseer un mayor control sobre la red veremos mecanismos mediante los cuáles se puede conseguir falsear llamadas y obtener información sobre las comunicaciones.

### Conclusiones y líneas futuras:

Tanto el analizador como la estación base son capaces de operar de forma eficaz dentro de las limitaciones que supone contar con equipos y software no concebidos para grandes infraestructuras. Pero estos desarrollos cuentan con la ventaja de basarse en código abierto y cuenta con muchas opciones para continuar añadiendo servicios y funcionalidades que pueden resultar útiles para empresas o centros educativos.

Para comprender el desarrollo realizado en los capítulos prácticos, es necesario conocer las características más importantes de las redes GSM. Durante el siguiente capítulo se tratarán de mostrar los protocolos, las unidades de información y los procedimientos de las redes móviles de segunda generación.

## Capítulo 2 – Estándar de telecomunicaciones GSM

## 2 Estándar de telecomunicaciones GSM

Se denominan redes de comunicaciones móviles a las redes de comunicaciones en las cuáles el receptor o el emisor, o bien ambos, se encuentran en movimiento. Por ésta razón, deben sustituir los interfaces cableados y utilizarse en su lugar el interfaz radio para la transmisión de información y señalización entre los interlocutores. Aunque desde mediados del siglo XX existían infraestructuras capaces de transmitir datos sin conexión física entre emisor y receptor, éstas contaban con tecnología demasiado cara y aparatosa. Por ello, los primeros sistemas de comunicaciones inalámbricos estaban únicamente al alcance de las fuerzas militares de los países más desarrollados.

Aunque en la actualidad la telefonía móvil está ampliamente extendida y existen redes en multitud de países, no sería hasta finales del siglo XX cuando aparecerían los primeros sistemas digitales comerciales. Pese a que el precio de los terminales, su tamaño y el costoso y difícil acceso a la red resultaban un impedimento para que el gran público accediese al servicio, se produjo una adopción tremendamente rápida. Esto provocó un rápido avance de la tecnología, que supuso una rebaja en el precio del acceso a los servicios móviles. En la actualidad, las empresas más poderosas del planeta, salvando a las petroleras, se dedican de forma directa o indirecta a las comunicaciones móviles.

### 2.1 Primeras redes de comunicaciones

La fabricación del primer radio teléfono corrió a cargo de la compañía Motorola en el año 1979 con la aparición de los primeros sistemas comerciales en Tokio, Japón, de la mano de la compañía NTT. La velocidad y la calidad de las transmisiones eran muy bajas y únicamente estaba contemplada la transmisión de voz. Además existía un gran problema de base para la primera generación de comunicaciones móvil y era la variedad de estándares existentes en los diferentes puntos geográficos dónde se estaban desarrollando. Existían tres tecnologías principalmente:

- TACS utilizado en Europa
- JTAC utilizado en Japón
- AMPS utilizado en América

Todas ésta implementaciones se realizaban sobre tecnología analógica y mediante conmutación de circuitos en todos los tramos de la comunicación. Aunque compartían ciertas características como la utilización de una división celular, la señalización en banda o las estaciones base terrestres, los estándares no eran compatibles entre sí por lo que los terminales que operaban en una red de Japón no podían conectarse a ninguna de las redes existentes en Europa.

Debido al incremento del uso de las redes ligado a su éxito comercial, se hizo necesario introducir cambios y nuevas características para mejorar las prestaciones de las tecnologías existentes. Los esfuerzos deberían centrarse en mejorar la eficiencia espectral de las comunicaciones, la interoperabilidad entre redes y la introducción de nuevos servicios como la transmisión de datos.

Como en muchos de los campos científicos, el principal problema era la falta de inversión para la investigación de nuevas soluciones o mejoras sobre las existentes. De esta manera, como el coste no podía ser asumido por un sólo país, varias

naciones europeas decidieron unirse para crear un nuevo estándar que buscase satisfacer los objetivos fijados.

En 1982 el *Groupe Spécial Mobile* dentro de la Conferencia Europea de Administraciones de Correos y Telecomunicaciones. Su función fue crear un estándar de comunicaciones móviles basado en tecnología digital que permitiese la interoperabilidad entre redes de diferentes países y operadores y evitase los problemas de las redes analógicas desplegadas anteriormente. Esto supuso el comienzo del estándar GSM que, aunque se trata del estándar de segunda generación, sería la primera red de telefonía móvil utilizada de forma masiva.

## 2.2 Redes GSM

El sistema global para las comunicaciones móviles (GSM), como se ha comentado anteriormente, se trata de un sistema estándar para la implantación de la telefonía móvil digital. Cualquier estación móvil puede conectarse y acceder a los servicios proporcionados por el operador de red entre los que se encuentran:

- Llamadas de voz
- Envío de SMS
- Acceso a Internet mediante GPRS
- Servicios de geolocalización
- Valores añadidos de la red (aviso de llamadas, buzón de voz...)

Quizás el mayor avance que introdujo la tecnología GSM fue la transición del mundo analógico al digital. La primera generación de comunicaciones móviles tenía grandes carencias motivadas, entre otros factores, por las limitaciones de los circuitos analógicos. Gracias al cambio de tecnología se consiguieron las siguientes ventajas con respecto a la generación anterior:

- Miniaturización de componentes y reducción del tamaño de los terminales y equipos de red
- Mayor capacidad de procesamiento y por tanto mayor inteligencia en los terminales y equipos de red
- Facilidad en el diseño y programación de los circuitos y componentes
- Mejora de la calidad y la fiabilidad de las comunicaciones debido a las codificaciones
- Utilización eficiente del espectro gracias a la mejora en la división de los canales y el ancho de banda

Otro de los grandes hitos del estándar GSM respecto a las tecnologías existentes en el momento, y que se sigue manteniendo en los nuevos estándares de comunicaciones móviles, es la utilización de la tarjeta SIM. Bien es cierto que las tarjetas han reducido su formato y aumentado sus capacidades de almacenamiento pero intrínsecamente siguen siendo muy similares a las primeras que se fabricaron. Las tarjetas SIM almacenan los siguientes datos reflejados en la Tabla 1 relativos al cliente.

Estas tarjetas posibilitan la compatibilidad de los terminales con los diferentes operadores y por lo tanto, permiten cambiar de operador sin cambiar de terminal. Además mediante los acuerdos de itinerancia entre operadores de diferentes países, es posible gracias nuestra tarjeta SIM, conectarse y operar en redes diferentes a la nativa. Algunos fabricantes de terminales móviles han intentado sin éxito eliminar la

utilización de las tarjetas SIM para tener un mayor control y ganar espacio extra en los terminales pero las operadoras se han negado [3]. Otra característica implementada por el estándar es el número de emergencias 112 válido a nivel mundial y de uso obligatorio para todos los operadores y fabricantes que utilizan el estándar GSM.

Código	Nombre	Significado
Ki	Authentication Key	Código de 16 bits para autenticar las tarjetas dentro de la red
ICCID	Integrated Circuit Card ID	18 dígitos que conforman un identificador único de cada tarjeta SIM
IMSI	International Mobile Subscriber Identity	Identificador de abonado dentro del estándar
MCC	Mobile Country Code	Código del país donde se encuentra la red
MNC	Mobile Network Code	Código del operador que gestiona la red

Tabla 1: Datos contenidos en la tarjeta SIM

En la actualidad se han implementado nuevas tecnologías más eficaces en la utilización del espectro y con velocidades de acceso mayores a las que proporciona el estándar GSM. Las redes denominadas UMTS o 3G son utilizadas por los terminales de última generación para acceder a internet con mayor velocidad, para acceder al correo electrónico o para conectarse a sus redes sociales preferidas mediante aplicaciones. En la actualidad, para el acceso a internet desde terminales avanzados (*smartphones, tablets...*), se utiliza principalmente ésta red aunque existen algunos escenarios en los que es necesario utilizar otras tecnologías. Por ejemplo, aunque la cobertura 3G está presente en la mayoría de las ciudades, en entornos rurales aún encontramos numerosas localizaciones donde no es posible acceder mediante ésta tecnología. En algunos casos, no tendremos más remedio que desplazarnos para conseguir comunicación pero las tecnologías de segunda generación (GPRS y GSM) aún cuentan con menor número de lugares en los que no está presente su cobertura. De todos modos, en algunos países ya se están empezando a instaurar las redes de la cuarta generación llamada LTE que promete velocidades incluso mayores que las de los puntos de acceso WiFi que tenemos actualmente en nuestros hogares. De todos modos ésta tecnología está en fase de pruebas en la mayoría de ISP y aunque los terminales más modernos la implementan, sólo es posible su utilización en determinadas ciudades y las tarifas aún son demasiado caras para el uso masivo.

Aunque en términos de velocidad las redes móviles de segunda generación se han visto superadas por las generaciones posteriores, siguen gozando de gran extensión en todo el mundo. Están presentes en más de 200 países y cuentan con más de 3000 millones de usuarios en todo el mundo, lo que hace que sea hoy por hoy la tecnología más usada por los terminales móviles. Además, los fabricantes y operadores siguen apostando ésta tecnología y tanto las tarjetas SIM como los terminales, implementan el estándar actualmente.

Para conocer el entramado de la red GSM, se expondrán a continuación las características más relevantes e innovadoras del estándar. Se hará especial hincapié en la interfaz radio por ser ésta la más importante y la que supuso el mayor avance para llevar la telefonía inalámbrica a millones de clientes a lo largo del planeta. Además se expondrán conceptos que permitirán al lector comprender de forma más sencilla las descripciones de los desarrollos realizados.

### 2.2.1 Interfaz Radio

Dentro de las redes GSM [4] existen dos partes bien diferenciadas dentro de lo que se denomina el interfaz físico. Por una parte, encontramos el interfaz radio, centrado en la utilización eficiente del espectro radioeléctrico y la división del recurso para ser usado por los diferentes proveedores de servicios, es decir, las directrices que definen cómo han de ser las señales electromagnéticas que circulan por el canal aéreo. Por otro la parte troncal de la red, que salvo en ubicaciones remotas, suele implementarse mediante cableado para proporcionar seguridad, fiabilidad y robustez a las comunicaciones. Se utilizan radioenlaces para unir puntos donde la instalación de cable es demasiado costosa o no se obtienen los permisos de ocupación de vía pública o privada.

### 2.2.1.1 Características físicas

En Europa por el año 1978 se decidió reservar la banda de los 900 MHz para las comunicaciones móviles. Posteriormente se utilizó también la banda de los 1800 MHz para disponer de mayor capacidad con un funcionamiento prácticamente igual al de las redes situadas en la banda de los 900MHz salvo por ciertas características físicas de las señales radio. Desde el nacimiento del estándar, el ITU [5] fijó una serie de frecuencias de uso para las redes GSM. Las principales bandas de operación se muestran en la Tabla 2, aunque podrían utilizarse para otras tecnologías radio.

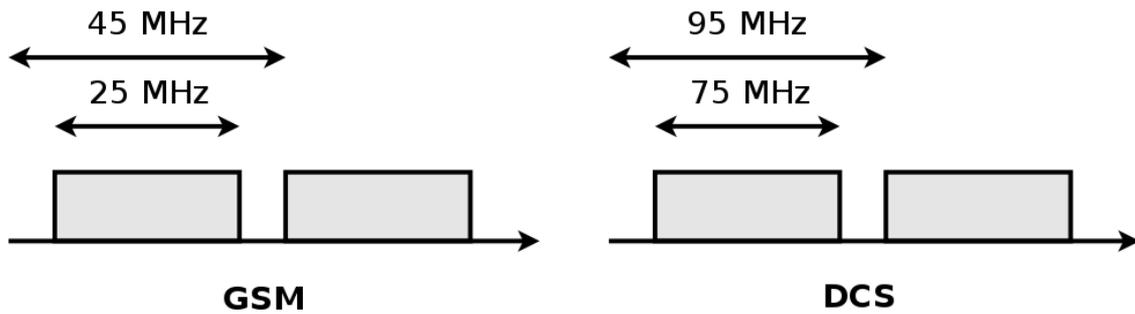
Banda	Nombre	Canales	Uplink (MHz)	Downlink (MHz)
GSM 850	GSM 800	128 - 251	842 - 849	869 - 894
GSM 900	P-GSM 900	0 - 124	890 - 915	935 - 960
	E-GSM 900	974 - 1023	880 - 890	925 - 935
	R-GSM 900	No disponible	876 - 880	921 - 925
GSM 1800	GSM 1800	512 - 885	1710 - 1785	1805 - 1880
GSM 1900	GSM 1900	512 - 810	1850 - 1910	1930 - 1990

Tabla 2: Bandas de frecuencias fijadas por el estándar GSM

El gobierno de cada país asigna el espectro radioeléctrico entre las operadoras que quieren ofrecer el servicio GSM dentro de sus fronteras. El mecanismo más común es el de concesión, mediante subasta pública de licencias de explotación durante un determinado periodo por cada país. Una vez que el operador adquiere su banda deberá dividir el mismo en multitud de canales diferenciados. Debido a que todas las comunicaciones comparten el mismo medio físico, es necesaria la multiplexación para que puedan realizarse varias de forma simultánea. La división se realiza con varias técnicas, la forma más común es la combinación de los siguientes modelos:

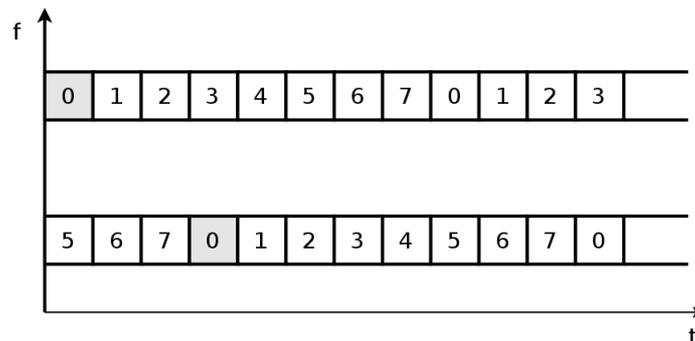
- División en tiempo: cada usuario transmite y recibe la señal en una determinada ranura temporal en la que no interfiere con los demás terminales.
- División en frecuencia: el envío y recepción se realiza a diferentes frecuencias para no interferir con las transmisiones simultáneas.
- División en espacio: el operador reutiliza el espectro de forma reiterativa entre celdas alejadas una distancia suficiente como para no interferir.

También se utilizan otras modalidades como salto aleatorio múltiple en frecuencia o *frequency hopping* con el fin de minimizar el ruido y la interferencia en las comunicaciones. Con éstas consideraciones se logran los diferentes canales que se conceden a cada usuario según su demanda así como canales de señalización y control de las comunicaciones.



**Ilustración 2: Distribución de canales en el estándar GSM**

El sistema GSM cuenta con duplexado en frecuencia por lo que cada canal de subida tiene su equivalente en bajada. Como puede observarse en la Ilustración 2, el ancho de banda ocupado por cada canal en la banda de 900 MHz es de 50 MHz, 25 MHz para subida y 25 MHz para bajada mientras que para la banda de 1800 MHz es de 150 MHz, 75 MHz para cada sentido de la comunicación. A modo de ejemplo, en la banda de los 900 MHz cada canal se subdivide en 124 canales de 200 KHz cada uno. No se utilizan los canales de los extremos porque, debido a la modulación de la señal, los canales ocupan 270 KHz en la práctica y se produciría *aliasing* fuera de la banda asignada. Cada uno de los 122 canales frecuenciales se divide a su vez en 8 *slots* temporales dando un total de 976 canales a nivel lógico. Nótese que existe un decalado entre las tramas (Ilustración 3) del *uplink* y *downlink* para permitir a los terminales y a la estación base el procesamiento de los datos antes de generar una respuesta.



**Ilustración 3: División y decalado temporal en GSM**

Para la división espacial, se heredó la partición celular de la telefonía analógica. Consiste en colocar cada una de las estaciones base en el centro de un hexágono, por similitud con círculo pero simplificando cálculos espaciales, con el fin de no superponer el área de influencia de una determinada frecuencia. De esta forma cada proveedor de servicios dispone las frecuencias en cada una de las celdas adyacentes creando un patrón que se repetirá a lo largo de cada país en el que esté presente. El factor de reuso de frecuencias viene dado por la calidad mínima que exige el estándar. Para células con mucha carga de usuarios se realizan divisiones más pequeñas que agrupan mayor número de frecuencias y por tanto de canales. Gracias a la división celular se dividen dichas entidades en sectores de  $120^\circ$  en incluso  $60^\circ$  para crear picoceldas en espacios reducidos con mucha demanda.

Agrupando varios de éstos *slots* temporales mencionados con anterioridad, se originan los canales lógicos. Estos contienen diferente información según el tipo. Transmisor y receptor han de tener en cuenta que al tratarse de canales cuya transmisión no es continua existen unos tiempos de espera y los equipos deberán ser capaces de almacenar las ráfagas anteriores para conformar una canal completo y dotar de sentido





### 2.2.1.4 Formato ráfagas GSM

La unidad básica de transmisión de información en el estándar GSM es una ráfaga. Cada ráfaga se transmite dentro de un *slot* temporal. Existen varios campos dentro de las ráfagas que contienen información muy variada. Los bits de información son propiamente los correspondientes al tráfico de usuario. Además se encuentran también secuencias de entrenamiento que permiten tanto a las estaciones como a los móviles realizar una estimación del canal y variar sus filtros para conseguir capaz la información con la mayor calidad posible. Estas secuencias son conocidas por ambos extremos y se utilizan para la ecualización del canal. Por último se encuentran los bits de cola, ceros lógicos situados al principio y al final para evitar la pérdida de eficiencia al demodular los bits útiles que transporta la ráfaga.

La ráfaga normal, mostrada en la Ilustración 7 contiene dos paquetes de 58 bits de información de usuario. Además entre ellos, se encuentra una secuencia de entrenamiento de 26 bits. La posición de la misma consigue minimizar la distancia entre extremos y mejora la reacción a variaciones del canal durante la transmisión de la ráfaga. Como contrapartida, al no ecualizar el canal al inicio de la comunicación, es necesario almacenar el primer paquete de 58 bits para poder posteriormente demodular correctamente la señal. GSM dispone de un total de 8 secuencias de entrenamiento conformadas de tal manera que la correlación entre las mismas sea mínima. Por último, se encuentran 3 bits en la cabecera y en la cola de relleno para facilitar el procesado.

Cola 3	Información 58	Entrenamiento 26	Información 58	Cola 3
-----------	-------------------	---------------------	-------------------	-----------

Ilustración 7: Ráfaga normal del estándar GSM

Un modelo diferente de ráfaga es la de acceso a la red. Es más corta de lo normal debido a que el móvil la emite sin conocer completamente la secuencia de tramas dentro de la estación base. Esto minimiza la probabilidad de colisión con otros dispositivos que campean en la misma celda. Se compone de un único paquete de información de 36 bits para enviar los parámetros de la petición de acceso. Como se puede ver en la Ilustración 8 se incluye, en este caso, una secuencia de entrenamiento de 41 bits para incrementar la probabilidad de demodular la señal correctamente ya que la estación base aún no conoce suficiente información sobre el terminal. También se compone de bits de relleno aunque para esta ráfaga el número de bits de cabecera es de 7.

Cola 7	Entrenamiento 41	Información 36	Cola 3
-----------	---------------------	-------------------	-----------

Ilustración 8: Ráfaga de acceso del estándar GSM

La ráfaga S sólo se utiliza en el enlace descendente para el canal SCH. Como el móvil desconoce los parámetros de la estación base, la secuencia de entrenamiento es de 64 bits ampliando la probabilidad de éxito en la demodulación. A ambos lados de la misma se sitúan paquetes de 39 bits de información que transmiten, como se vio anteriormente, la configuración de la estación base.

Cola 3	Información 39	Entrenamiento 64	Información 39	Cola 3
-----------	-------------------	---------------------	-------------------	-----------

Ilustración 9: Ráfaga S del estándar GSM

El último tipo es la ráfaga F. Es la más sencilla ya que consta de 148 bits, todos ellos ceros lógicos. Gracias a la modulación utilizada en GSM, ésta ráfaga es una señal sinusoidal pura y permite a los terminales móviles encontrar de forma sencilla la frecuencia guía de las estaciones base que emiten a su alrededor.

## 2.2.2 Red troncal

La red troncal GSM hereda de la red RDSI que ya estaba desplegada por la mayoría de operadores para la prestación de servicios de telefonía y datos en ubicaciones fijas. A partir de este punto se comparte la infraestructura existente y se utilizan las interfaces implementadas anteriormente. Al igual que las redes RDSI, se basa en conmutación de circuitos por lo que los usuarios disponen de canales dedicados exclusivamente para cada comunicación. No será hasta la siguiente generación, conocida como 3G, cuando se introduzca la conmutación IP que utiliza los recursos de forma balanceada entre los usuarios que necesitan acceso a la red.

Más adelante, cuando se hable de la topología de las redes GSM, se mostrará el punto de interconexión que separa la interfaz radio, las nuevas interfaces para estaciones móviles y la interconexión con la fija de datos existente antes de la implantación de las redes móviles de segunda generación.

## 2.2.3 Arquitectura de las redes GSM

La arquitectura GSM se divide en cuatro grandes bloques o subsistemas. Cada uno de ellos realiza una función dentro de la red. El estándar sólo especifica los componentes y su interconexión, queda en manos del operador de la red la forma de implementación de los mismos. Los subsistemas son los siguientes:

- MS: Mobile Station o Estación Móvil
- BSS: Base Station System o Subsistema de Estación Base
- NSS: Network and Switching System o Subsistema de Red y Conmutación
- OSS: Operation Support System o Subsistema de Operación y Mantenimiento

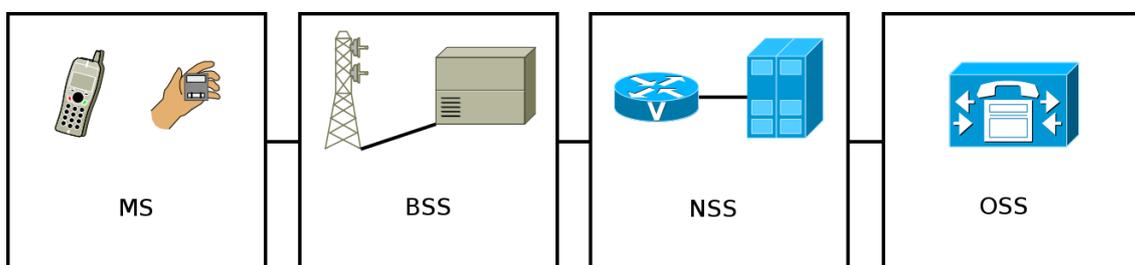


Ilustración 10: Arquitectura de red GSM

Cada uno de ellos engloba una serie de elementos y sus funcionalidades para realizar comunicaciones según el estándar. La comunicación entre los elementos se realiza mediante las interfaces que se muestran en la Ilustración 10 y en ambas direcciones según el sentido de la comunicación. Comenzaremos introduciendo los elementos que conforman la arquitectura GSM inicial y posteriormente veremos los añadidos para GPRS.

### 2.2.3.1 Estación móvil

Las funciones propias de la estación móvil son el acceso a la red GSM a través del interfaz radio y el establecimiento de un interfaz de usuario para las comunicaciones de voz y datos.

En primer lugar encontramos el terminal móvil. Existen multitud de ellos así como de formas de clasificar a los mismos. Ejemplos pueden ser su potencia emitida, sus características, los servicios añadidos soportados... Los terminales son proporcionados por un fabricante externo pero es necesario adquirir una tarjeta SIM par conectarse a una red y acceder a los servicios proporcionados por la misma. Algunos operadores ofrecen subvención de los terminales a cambio de permanencia en el contrato adquirido por el acceso al servicio. Estos terminales únicamente pueden ser utilizados con una SIM del operador que los oferta, de todos modos, es posible adquirir terminales ofrecidos directamente por el fabricante y que aceptan tarjetas SIM de cualquier operador. Actualmente es uno de los sectores de mayor beneficio dentro de la electrónica de consumo.

Como se expuso al principio del capítulo, la tarjeta SIM es uno de los elementos más importantes del estándar GSM y que sigue presente en las nuevas generaciones de sistemas de comunicaciones móviles. Existen actualmente diferentes modelos (microSIM, nanoSIM...) difiriendo únicamente en el tamaño pero manteniendo las funcionalidades originales. La tarjeta contiene todos los datos necesarios así como las claves de seguridad necesarias para identificar al usuario dentro de la red. Los códigos presentes en las tarjetas se han mostrado al inicio del capítulo en la Tabla 1.

Además poseen un espacio de memoria adicional en el que pueden almacenarse datos como directorio telefónico o aplicaciones e información adicional del operador (números de información, acceso al buzón de voz...).

En las primeras pruebas también se diferenciaban diferentes elementos software y hardware dentro de los terminales pero en la actualidad no es relevante su definición puesto que se encuentran totalmente integrados dentro de la estación móvil y son totalmente transparentes al usuario.

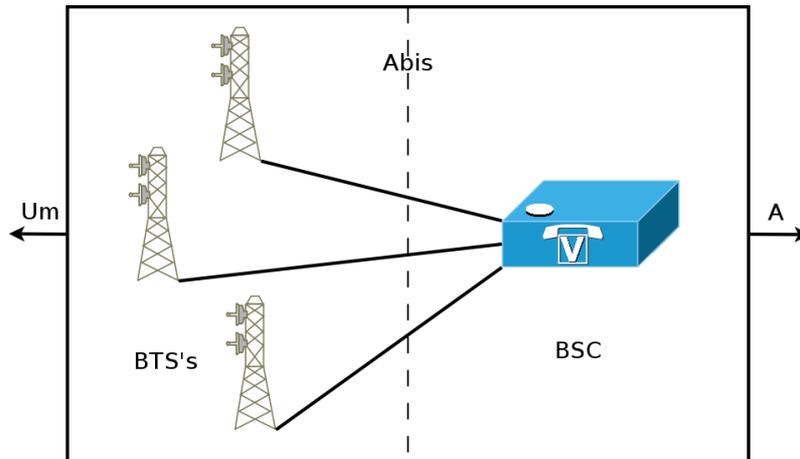
### 2.2.3.2 Subsistema de estación base

Este bloque se compone de dos elementos principales: las estaciones base (BTS) y las controladoras de dichas estaciones (BSC). Implementan prácticamente la totalidad del control de interfaz radio y son las encargadas de interactuar directamente con las estaciones móviles.

Las interfaces de conexión con el resto del sistema son por un lado la Um que permite dialogar y transmitir la información de tráfico a los terminales que campean en la celda y por otro el interfaz A con la MSC que explicaremos a continuación. El interfaz que une las BSC's con las BTS's se denomina Abis.

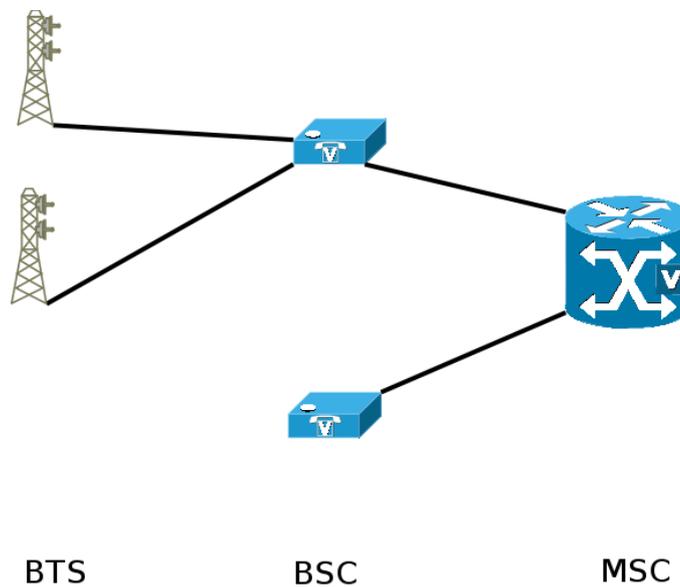
Las BTS abarcan todos los dispositivos necesarios para la transmisión y recepción radio del sistema GSM incluyendo las antenas (Ilustración 11). El cometido de las BTS es conformar la señal radio para su transmisión y realizar la recepción correcta de las señales entrantes. Realizan el procesado de las señales, su codificación, el entrelazado de los bits... Normalmente contienen antenas omnidireccionales y se colocan en el centro de la celda. La potencia máxima de transmisión determina el

tamaño de la misma. Una BTS puede tener un máximo de 12 transceptores (TRx) que emiten en cada una de las frecuencias del operador en la celda.



**Ilustración 11: Subsistema de estación base**

Por encima de las BTS se encuentran las BSC que agrupan varias de las mismas. Además de la gestión de las BTS que dependen de ella, la controladora de estaciones base se encarga de gestionar la asignación de recursos radio. Su labor consiste en liberar y conceder canales para las diferentes comunicaciones así como los trasposos de llamada siempre que se produzcan entre BTS's dependientes de la misma BSC. También controla el cifrado de los datos y gestiona algoritmo de eficiencia de las comunicaciones como puede ser la transmisión de ruido de confort ante los silencios producidos en las comunicaciones.



BTS

BSC

MSC

**Ilustración 12: Interconexión del BSS con el NSS**

En el otro lado de la comunicación se encuentra el MSC que controla varias BSC's y se encarga de encaminar las llamadas hacia la red. La BSC es la encargada de controlar en todo momento las comunicaciones por lo que tanto el terminal móvil como la BTS informan periódicamente del estado de la comunicación y de los parámetros relevantes para la misma. Por ejemplo, el móvil envía información sobre la potencia que recibe de las estaciones base adyacentes y la BSC procesa la información para decidir si es necesario un traspaso según criterios preestablecidos.

Por último se encuentra también la unidad TRAU. El estándar no establece una ubicación fija de la misma por lo que puede encontrarse indistintamente en la BTS, en la BSC o en el MSC. Su cometido es adaptar los diferentes regímenes de transmisión. La velocidad de transmisión de los terminales móviles es de 16 kbps y debe ser adaptado a los 64 kbps de transmisión de la RDSI utilizada en el *backbone*.

### 2.2.3.3 Subsistema de red y conmutación

Hablaremos ahora del sistema de enrutamiento del estándar GSM. El NSS se encarga de redirigir las llamadas generadas por los usuarios en los tramos anteriores bien dentro de la propia red de un determinado operador o hacia las redes de los diferentes operadores. Se ha de tener en cuenta que independientemente de los operadores que gestionen las redes a las que va dirigido el tráfico, éstas pueden ser móviles pero también fijas indistintamente.

Esta parte del sistema se encarga también de gestionar las diferentes bases de datos existentes para su correcto funcionamiento. Dichas bases de datos contienen información de distinta naturaleza sobre los abonados: claves de autenticación y cifrado, tipos de tarifa, números identificativos...

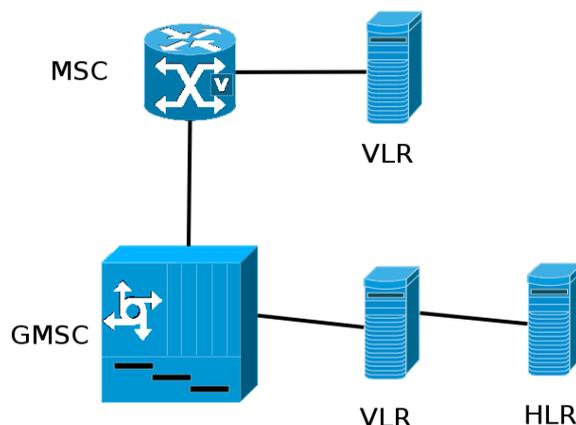


Ilustración 13: Subsistema de red y conmutación

Como se observa en la Ilustración 13, existen dos tipos de centrales de conmutación dentro del subsistema: MSC y GMSC. La primera (MSC) es la central de conmutación interna de la subred del operador. Por su parte, la GMSC conecta la red del operador con las diferentes redes destino y sirve como puerta de enlace hacia las redes destino.

Encontramos además dos bases de datos. El HLR es el registro general de abonados que contiene información acerca de todos los abonados que pertenecen a la red de un determinado operador, mientras que el VLR contiene información más extensa pero únicamente de los abonados localizados en un área determinada.

El HLR contiene toda la información sobre los abonados registrados en la red del operador correspondiente. En sus inicios, los operadores sólo mantenían una base de datos general pero ante el incremento del número de abonados, en la actualidad se mantienen varias bases de datos repartidas estratégicamente para controlar de forma eficiente la información sobre los mismos. Alberga información permanente y temporal. Entre la información permanente se encuentran todos los identificadores del abonado y del terminal así como los servicios contratados y sus tarifas, mientras que la ubicación, la tarificación actual, claves de autenticación y cifrado de las

comunicaciones... se almacena de forma temporal. Queda a elección del operador la forma en la que se gestionan estas bases de datos y cómo se implementa el sistema para utilizar los recursos de manera eficiente buscando evitar duplicar la información en la menor medida posible y establecer métodos de búsqueda de abonados que no penalicen el funcionamiento.

El VLR por su parte, contiene una versión simplificada de la información contenida para cada abonado en un área determinado en el HLR. A ésta se añade la ubicación geográfica exacta del terminal para establecer su posición dentro de la red GSM.

Para realizar la comunicación entre los diferentes elementos del subsistema se recurre a SS7 que se trata de un estándar de señalización fuera de banda ampliamente utilizado por otros sistemas de comunicaciones. De ésta manera se reutilizan protocolos ya existentes y se simplifica la interconexión entre los elementos anteriormente citados.

A modo de ejemplo, imaginemos una llamada entrante que se produce en una red, fija o móvil, de un operador diferente al de destino. La llamada llegará primero al elemento GMSC que se encuentra en la frontera de conexión con el exterior. La primera acción a realizar por el *gateway* será encuestar a la base de datos general, HLR, sobre la ubicación del terminal móvil al que va dirigida la comunicación. Una vez conocida la ubicación del MSC que está presentado servicio al abonado, se encaminará la llamada hacia el mismo. Entonces, se buscará dentro del VLR estación base en la que campea el destinatario. En dicho registro se encuentran todos los datos necesarios para localizar al terminal y enviar la llamada entrante.

#### 2.2.3.4 Subsistema de operación y mantenimiento

Como casi cualquier sistema de red, GSM también necesita de mecanismos y equipos que velen por la seguridad y el correcto funcionamiento de la red y los servicios que ofrece la misma. Además deben existir mecanismos que permitan modificar comportamientos y parámetros de configuración en tiempo real para prevenir y reparar cualquier comportamiento anómalo del sistema. Las redes GSM han crecido mucho desde su implementación y es vital disponer de una plataforma de gestión remota para poder gestionar redes de grandes dimensiones.

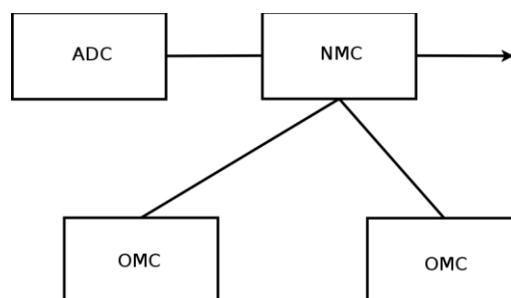


Ilustración 14: Subsistema de operación y mantenimiento

Existen tres dominios de gestión para cada uno de los equipos gestionados:

- Centro de Operación y mantenimiento: Se trata de la interfaz mediante la cual el humano puede interactuar con el sistema para modificar parámetros, monitorizar los recursos...

- Control de la subscripción: Contempla la gestión de los datos de abonado así como la tarificación. El estándar no es nada específico en este apartado y los operadores pueden decidir su forma de implementación.
- Operación y mantenimiento: Engloba todas las funciones que se pueden realizar sobre la red y su configuración así como la gestión de las estaciones de base y los equipos electrónicos presentes en la infraestructura de red.

El elemento principal del subsistema de gestión es el NMC. Se encarga de gestionar la totalidad de la red propia del operador además de todos los aspectos relacionados con la interconexión a redes externas. Obtiene información a través de multitud de OMC colocados en las zonas/equipos a monitorizar y/o configurar. Al tratarse de redes de telecomunicaciones, la gestión se realiza de forma remota de modo que es posible realizar grandes configuraciones en equipos lejanos sin necesidad alguna de desplazarse a la ubicación de los equipos implicados.

## 2.3 GPRS

Una vez que el sistema GSM estaba asentado y ampliamente extendido alrededor de todo el mundo, surgieron nuevas necesidades dentro de la red. El auge de Internet y la necesidad de transmisión de datos de forma inalámbrica propiciaron que se añadiesen elementos y protocolos a las redes GSM existentes para dotarlas de estos servicios. Aunque no se trata de una nueva generación de telefonía móvil se conoce a GPRS como la generación 2,5G. Por lo tanto esta tecnología se establece como un sistema complementario a GSM y ambos estándares comparten los mismos canales radio repartiendo los recursos disponibles según la demanda.

Aunque GSM fue concebido para la transmisión de voz mediante conmutación ante la demanda se nuevos servicios se realizaron pequeñas modificaciones, aprovechando su carácter digital, para conseguir la transmisión de datos a baja velocidad mediante conmutación de paquetes. De esta manera, los canales radio para la transmisión de datos son compartidos por varias comunicaciones y no se utilizan de manera exclusiva para cada comunicación. Debido a la tasa de transmisión no constante de las comunicaciones de datos esta técnica resulta más eficiente y permite albergar nuevos servicios de acceso a internet, posicionamiento, alertas... Además la nueva naturaleza de las comunicaciones permite la tarificación por volumen de información, agrupada en paquetes de datos, en lugar de por tiempo de conexión como se venía haciendo para los servicios de voz.

### 2.3.1 Arquitectura GPRS

La interfaz GPRS permite la transferencia de datos mediante conmutación de paquetes a través del canal radio entre el usuario final y las redes de datos convencionales como pueden ser X.25 o IP. El estándar define la interconexión con redes de datos de distinta naturaleza así como con las redes GPRS pertenecientes a diferentes operadores.

GPRS introduce dos nuevos elementos dentro de la arquitectura GSM existente hasta el momento que operan de forma complementaria los elementos explicados anteriormente (Ilustración 15). Se trata de entidades que tienen sus iguales en la infraestructura anterior pero que operan de manera independiente a los mismos cuando se trata de comunicaciones de datos. Si en GSM el encargado de realizar la

conmutación de circuitos era el MSC, GPRS añade un elemento paralelo llamado SGSN que en este caso realiza la conmutación de paquetes. Del mismo modo, si la interconexión con otras redes de voz era el GMSC quien lo realizaba, su función equivalente para la conexión con redes de datos externas se realiza mediante el GGSN.

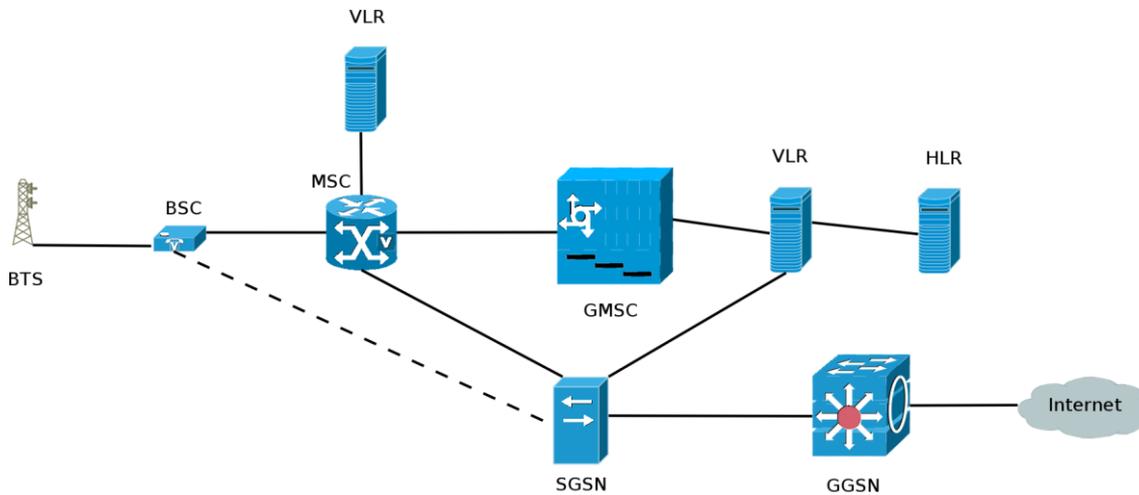


Ilustración 15: Arquitectura de redes GSM con servicio GPRS

Los elementos de gestión de recursos radio BTS y BSC, no sufren modificaciones de su arquitectura sino que se añaden nuevas funcionalidades dentro de los mismos que posibilitan el uso compartido de los canales así como los nuevos procedimientos y protocolos que introduce GPRS. También se comparten por ejemplo las bases de datos HLR y VLR que simplemente amplían la información contenida y su funcionalidad para poder dar soporte a los nuevos servicios.

El nodo SGSN se encarga básicamente del control de acceso al sistema, seguridad y localización de los terminales dentro de la red. El interfaz conocido como Gbis comunica el nodo con el BSS y posibilita el diálogo con el terminal móvil. Cuando un terminal desea acceder a los servicios GPRS se establece un procedimiento conocido como GPRS *attach* que tiene como resultado la creación de un contexto entre el SGSN y el terminal. Desde ese momento el terminal podrá iniciar una conexión de datos en cualquier momento y además se mantendrá monitorizado por el sistema para conocer su posición a fin de hacerle llegar la información que solicite.

El elemento GGSN realiza funciones de conexión con otras redes de datos basadas en conmutación de paquetes pero de diferente naturaleza como pueden ser redes X.25, IP, etc... Se encarga de gestionar el mapeado de direcciones para realizar el encaminamiento de los paquetes que se generen entre el terminal móvil y las redes externas a través de SGSN y GGSN. Como GSM no fue concebida para la transmisión de datos, el enrutamiento interno dentro de la red GPRS se realiza mediante túneles entre nodos. Se establece por una parte un túnel entre el terminal móvil y el SGSN y otro entre el SGSN y el GGSN que están prestando servicio a la comunicación.

Debido a la limitación de los primeros terminales compatibles, se establecen 3 clases: A, B y C. Los terminales de clase C sólo pueden acceder a los servicios GSM y GPRS de forma excluyente, es decir, necesitan desactivar uno de ellos para poder acceder al otro. Por lo tanto, no podrían estar a la espera de una conexión de datos y de voz a la vez sino que siempre deberán escoger una de ellas. Para los terminales de clase A y B si es posible mantenerse a la espera de cualquier tipo de comunicación pero únicamente podrán tener establecidas conexiones de ambos tipos al mismo tiempo los de clase A.

### 2.3.2 Enrutado de los paquetes

Una de las diferencias más destacadas dentro de la tecnología 2G y 2.5G fue el cambio del modo de enrutar las comunicaciones. Debido al cambio en la estrategia de conmutación, la forma de dirigir los paquetes de datos tuvo que ser renovada al no poderse reutilizar la manera en la que se establecían las sesiones de voz. Dentro del enrutado de paquetes existen tres escenarios posibles: entre terminal móvil y red externa, entre terminal móvil y otra red GPRS y entre terminal móvil y la misma red GPRS del operador.

Las unidades de información, conocidas como paquetes, se conocen como PDP PDU. PDP es el protocolo utilizado para establecer las sesiones de datos, es decir, después de un GPRS *attach* (mecanismo de conexión de abonados a la red de paquetes GPRS) se establece lo que se denomina un contexto PDP entre el terminal y GGSN o lo que es lo mismo, una sesión entre ambos donde el terminal está preparado para recibir o enviar datos y el GGSN monitoriza el terminal para que pueda hacerlo. En el caso de la comunicación entre terminal y SGSN se utiliza un protocolo creado específicamente para la especificación GPRS. Cuando este tiene que enviarlo hacia el GGSN se realiza el envío sobre TCP/IP a través de túneles separando de esta forma las comunicaciones de los diferentes servicios.

Los elementos SGSN y GGSN realizan también tareas de reenvío de información, una especie de routers que reciben paquetes por uno de sus puertos o enlaces y los envían por la salida correspondiente. Si éste reenvío no es posible cuenta además con *buffers* que permiten su almacenamiento hasta que puedan ser reenviados. El sistema GPRS transporta, a través de sus nodos y las diferentes interfaces, las unidades de información PDP PDU entre los terminales móviles y las redes externas de forma transparente. Para ello, las tramas son encapsuladas y enviadas a través de túneles respetando el contexto PDP entre el terminal y el GGSN.

## 2.4 Implementación de sistemas GSM

Una vez conocidos los procedimientos y sistemas existentes en el estándar GSM, se realizará un primer estudio de las soluciones existentes para implementar y monitorizar una red. Esto será determinante a la hora de escoger la más adecuada a nuestras necesidades y a los medios técnicos y económicos con los que contamos. Los sistemas que se han desarrollado distan de los que existen de manera comercial y que implementan operadores y fabricantes. Se indicará posteriormente la manera en la que se realizan las implementaciones actualmente con los equipos y tecnologías disponibles en el mercado.

### 2.4.1 Implementación de estaciones base GSM

A continuación se explicarán a grandes rasgos los procedimientos y costes que acarrea la implementación de una estación base dentro de un sistema GSM. No se tendrá en cuenta el proceso y los costes derivados de la elección y el estudio de la ubicación de la estación, el estudio del tráfico potencial y de los estudios anteriores a su implementación. Nos centraremos principalmente en los componentes que se ubican en la estación base: BTS y BSC. De la misma manera se realizará la comparación entre las soluciones comerciales y otras realizadas mediante software libre.

Para simplificar el ejemplo, no se tendrá en cuenta el coste de las licencias necesarias para operar dentro de las bandas de frecuencia licenciadas en cada país aunque se ha de tener en cuenta que es la parte dónde los operadores desembolsan gran cantidad de su capital para adjudicarse las bandas necesarias para implementar sus sistemas. Éste gasto no se diferencia aunque la forma de ofrecer el servicio sea mediante plataformas abiertas utilizando software con licencias libres ya que el interfaz radio siempre es el mismo independientemente de la tecnología que se utilice en su implementación.

Ha de tenerse en cuenta que queda fuera del análisis el alto coste de las licencias que se pagan por el uso de las bandas de espectro radioeléctrico que han sido adquiridas por los operadores y que no pueden ser utilizadas por otras implementaciones. Recordemos que el uso previsto para la estación base se restringe a entornos reducidos como puede ser un laboratorio. Si el alcance de la cobertura que proporciona la antena llegase a zonas públicas o de terceros podríamos incurrir en un delito fuertemente penado por las leyes estatales. Otro de los gastos más elevado para los operadores es la electricidad necesaria para mantener en funcionamiento los equipos instalados en cada una de las estaciones base así como en las centrales de conmutación de la parte de troncal de la red. No se especificará en esta comparación ya que se trata de un gasto recurrente difícilmente medible, aunque en el caso de los operadores convencionales los datos indican que supone una parte muy importante del presupuesto de las compañías para mantenimiento de la infraestructura. En las soluciones abiertas el gasto a priori resulta bastante más reducido debido a que se puede conseguir una celda totalmente funcional con un PC estándar, un router comercial de gama media-baja y un equipo radio cuyo consumo podría aproximarse al de 3 PC's corrientes. De todos modos, no resultaría objetivo comparar la implementación pretendida con las soluciones realizada por los grandes operadores ya que la dimensión y las capacidades de las redes son inmensamente mayores en este último caso. La mayor ventaja con la que cuentan las soluciones abiertas realizadas mediante código libre es precisamente su naturaleza no restrictiva. Esto posibilita un control total sobre la red y la posibilidad real de conseguir mejoras. Por último, también se excluirá del análisis el gasto correspondiente a la utilización de redes externas. Dicho gasto en el caso de las implementaciones comerciales, se debe a las tasas a pagar por la utilización de equipamiento de otras compañías cuando se realizan llamadas entre terminales con diferentes proveedores de servicios. Los acuerdos entre empresas no son de dominio público y cuentan con muchas variantes por lo que no es posible especificar su la cantidad exacta a pagar por un determinado operador. Para el caso de las implementaciones abiertas el coste se deriva del acceso a internet necesario para conectar con otras redes de comunicaciones cuyas tarifas son muy variadas.

Así pues, para que exista la máxima similitud entre los casos propuestos, supondremos que los equipos emisores sólo lo harán en una única frecuencia base y se fijará como suposición que el número de usuarios potenciales puede ser gestionado por una sola antena produciéndose la congestión a partir del mismo número de llamadas simultáneas en ambos casos. En las condiciones citadas, el primer desembolso que debe realizar un operador para instalar una celda GSM es la compra/alquiler del terreno. El precio a pagar puede ser muy variado según la situación y las negociaciones. En comparación, los equipos a instalar en las soluciones abiertas, se ha de comentar que el espacio ocupado por los equipos es mínimo por lo que 1 metro cuadrado es suficiente para su ubicación. Bien es cierto, que para cualquiera de los casos es necesario dotar a la instalación de suministro eléctrico suficiente para que puedan operar los equipos así como armarios o carcasas aisladas de forma correcta para poder soportar inclemencias atmosféricas. Como se ha comentado, las soluciones implementadas mediante software libre son más baratas

debido a que los equipos consumen menos potencia y las carcasas de los mismos son más pequeñas.

En la actualidad, los equipos comerciales cuentan con software que gestiona el equipamiento y dicho software es en gran parte licenciado por los fabricantes del propio hardware. Las soluciones libres se implementan mediante software de licencia abierta por lo que no es necesario incurrir en gasto alguno para poder hacer uso del mismo. Eso sí, el soporte ante cualquier problema de funcionamiento o configuración no está garantizado debido a que se lleva a cabo por lo propios usuarios mediante wikis, foros o listas de correo. Aunque en principio supone un inconveniente para sistemas comerciales críticos que dependen fuertemente de la calidad del servicio (disponibilidad, tolerancia a fallos, etc...) puede verse como una ventaja debido a que puede modificarse según las necesidades debido a que el código está disponible de forma libre.

Por último, para incluir una comparación cuantitativa, un operador estándar debería desembolsar unos 200.000 dólares para implantar su red en una zona rural sin cobertura, lo que daría cobertura a unos miles de personas en un radio de unos 15 kilómetros, pero además habría que utilizar generadores diésel que elevarían el coste de unos 12 a 18.000 dólares al mes. En el caso de las soluciones abiertas, es posible instalar una estación base completamente operativa con un desembolso de poco más de 3.000 dólares para adquirir una BTS y un PC que controle la misma así como un elemento de conexión con la red telefónica conmutada e internet. Además, al tratarse de elementos que no consumen mucha potencia, se podrían alimentar mediante paneles solares u otras que no tendrían gastos recurrentes.

#### 2.4.2 Implementación de analizadores de redes móviles

Existen en la actualidad multitud de sistemas para realizar medidas dentro de las frecuencias relativas a las comunicaciones móviles. Su calidad y precio varían en función del rango de frecuencias soportado y la sensibilidad de medida que sean capaces de alcanzar. Mientras mayor sea su sensibilidad, el precio se incrementará al igual que mientras mayor sea el rango de frecuencias y más altas sean las mismas. La mayoría de los equipos comerciales que comprenden el rango espectral de las comunicaciones móviles terrestres, son capaces además de analizar otras emisiones como las de televisión y las bandas libres utilizadas para radioenlaces o WiFi.

Fabricante	Modelo	Rango frecuencial	Resolución de ancho de banda	Funciones añadidas	Precio
GW Instek	GSP830	9 KHZ - 3 GHz	3 KHz	Salidas VGA y USB	4860 \$
Tektronix	SA 2600	10 KHz - 6.2 GHz	10 Hz	Portátil, datos exportables a CSV y MATLAB	24579 \$
Aeroflex	3254/0	1 KHz - 26.5 GHz	3 Hz	Gestión remota basada en Windows XP	Desde 29744 \$

Tabla 3: Comparativa de equipos analizadores de redes Wi-Fi

Como se puede observar en la Tabla 3, el incremento de precio se corresponde con los criterios establecidos. De todos modos, el segundo equipo incrementa en gran medida su precio al tratarse de una estación de medida portátil de reducidas dimensiones y que debe utilizar baterías.



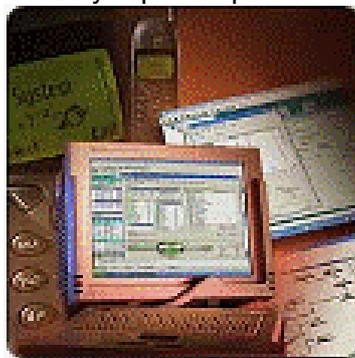
**Ilustración 16: Ejemplos de analizadores comerciales**

Hasta ahora hemos hablado de equipos capaces de realizar medidas dentro del espectro radioeléctrico. Los equipos son capaces medir características físicas de las emisiones, generar reportes, mostrar gráficos temporales/frecuencias, pero por sí mismos no son capaces de interpretar la información transportada por la radiofrecuencia que analizan.



**Ilustración 17: LTE Smart Analyzer de RADCOM**

Para encontrar un sistema que integre todas las funciones necesarias para la captación e interpretación de la información transportada en las comunicaciones móviles terrestres hay que recurrir al producto eDiamond LTE Smart Analyzer [7] de RADCOM (Ilustración 17). Éste producto es capaz de captar señales de todos los estándares de comunicaciones móviles digitales (GSM, UMTS y LTE). Además puede colocarse en cualquier punto de la red y es capaz de captar cualquiera de las comunicaciones (siempre claro está, que no sea cifrada). Como añadido, implementa funciones para generar estadísticas y reportes periódicos.



**Ilustración 18: Analizador GSM K15 de Tektronics**

**Otro producto similar que permite analizar protocolos entre los cuáles se encuentran los de segunda generación de móviles es el modelo K15 [8] de Tektroniks (**

). Permite además analizar protocolos 3G mediante una interfaz gráfica y obtener múltiples reportes sobre rendimiento y funcionamiento de la red. Además del tráfico puro de datos permite analizar los protocolos de codificación de la voz así como los protocolos de señalización SS7 utilizados en el control de las comunicaciones. Permite la traza de varias llamadas simultáneas en tiempo real y además al adquirir el producto se ofrece soporte completo sin coste añadido.

No se ha tenido acceso al precio de venta ya que es necesaria la solicitud mediante presupuesto indicando la utilidad que se obtendrá del mismo. Algunas empresas que poseen éstos equipos en propiedad ofrecen los mismos en alquiler para realizar determinadas pruebas sin necesidad de obtener el producto.

## Capítulo 3 – Estado del arte en redes móviles

## 3 Estado del arte en redes móviles

Actualmente la tecnología GSM es la más utilizada para establecer comunicaciones móviles terrestres alrededor de todo el mundo y está presente en más de 200 países. Además cuenta con el mayor número de equipos y dispositivos compatibles con la misma ya que a pesar de que las nuevas generaciones de telefonía ofrecen mayor calidad, velocidad y eficiencia en sus servicios, los terminales que se fabrican hoy en día siguen siendo compatibles con GSM. Es necesario destacar además que existen determinadas zonas, especialmente en medios rurales, que aun no cuentan con cobertura de tercera generación y es necesario que los terminales mantengan retrocompatibilidad para permitir la conexión de esas poblaciones.

### 3.1 Despliegue de redes móviles en España

La implementación de servicios de redes móviles en el territorio español está controlada por el Ministerio de Industria, Energía y Turismo [9]. Debido a que el recurso necesario para la explotación de las comunicaciones móviles terrestre es el espectro, el órgano anterior realiza concesiones por determinados periodos temporales a las empresas que quieren entrar en el negocio. Los dos primeros operadores que ofrecieron GSM de forma comercial dentro de España fueron Telefónica, la actual Movistar, y el consorcio Airtel-Sistelcom-Reditel, la actual Vodafone). Para conocer el estado actual de la adjudicación de licencias de explotación es necesario remontarse a las primeras subastas. Dichas adjudicaciones se realizan por un número determinado de años por lo que han sufrido variaciones con cada nueva subasta. Actualmente se encuentran vigentes para la explotación comercial bandas de 2G, 3G y recientemente de 4G.

#### 3.1.1 Subasta de bloque dentro de las bandas de frecuencia

Telefónica y Vodafone adquirieron por subasta la concesión de dos sub-bandas frecuenciales, cada una, dentro de la banda de los 900 MHz para el despliegue de su negocio mediante tecnología GSM en el 3 de Febrero del año 1995 y con vigencia hasta el mismo día del año 2020. Posteriormente, en el 24 de Julio de 1998 se concedieron dos nuevas sub-bandas frecuenciales en la banda de los 1800 MHz a Telefónica y a Vodafone además de a France Telecom que entró en el negocio con su filial Amena. Debido a la saturación por aquel entonces de la banda de 900 MHz, Amena, que sería adquirida por Orange, únicamente poseía frecuencias altas. Esto le situaba en una desventaja competitiva ya que dichas frecuencias penetran peor en los edificios y tiene un radio de alcance menor por lo que se veían obligados a instalar un mayor número de antenas. Además el consumo energético de los chips de comunicaciones situados en terminales y estaciones bases es mayor en frecuencias altas.

Ya en el año 2005 tras la liberación de bloques de frecuencia en el entorno de los 900 MHz se adjudicaron 6 canales a France Telecom que pasaría a tener el mayor número de frecuencias en dicha banda. La adjudicación, como en el caso de los otros operadores, finalizará en el año 2020. Estas frecuencias asignadas se reservaban únicamente para la explotación del sistema GSM. Para la telefonía UMTS o de tercera generación se había realizado la subasta en el año 2000 aunque en aquellos años la tecnología no estaba madura. Vodafone, Telefónica y France Telecom se hicieron con

3 bloque en la banda de los 2100 MHz a los que se añadió una compañía llamada Xfera Móviles que adquirió otros 3 bloques de frecuencias. La distribución hasta entonces de las frecuencias quedaría como se muestra en la Ilustración 19.

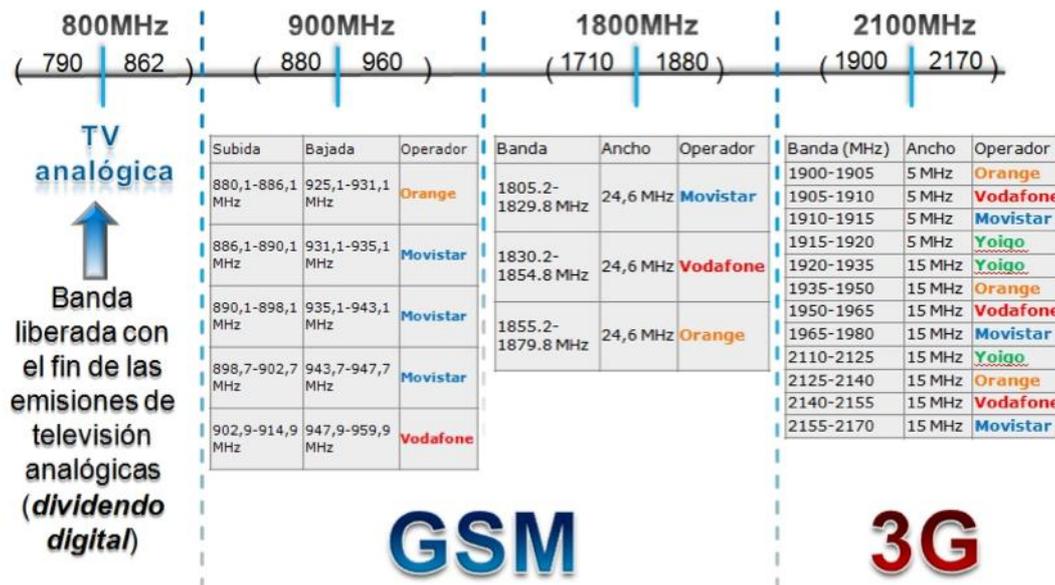


Ilustración 19: Mapa de bandas de frecuencia de telefonía en España

La última subasta del espectro [10] comenzó el 7 Julio de 2011 y tras 22 jornadas finalizó con una recaudación total para el Estado de 1.647 millones de euros. Se realizó para adjudicar licencias de explotación de la tecnología LTE en la banda de los 2,6 GHz que estarían disponibles al final de la misma. Además, debido al denominado dividendo digital, también se subastaron bloques en la banda de los 800 MHz que quedarán libres en 2014 por la migración de la Televisión Digital Terrestre. Los tres grandes operadores: MoviStar (Telefónica), Orange (France Telecom) y Vodafone, adquirieron bloques en ambas bandas con una inversión de 668, 437 y 518 millones de euros respectivamente. Además entraron en la puja, aunque sólo supuso 2,5 % del desembolso total, operadores que prestaban su servicio a través de la infraestructura de los tres grandes como son JazzTelecom, Euskaltel u ONO, y otros nuevos como R, Telecable o Telecom Castilla La Mancha. En éste caso quedaron libres algunas frecuencias que en principio serían adquiridas por Yoigo pero el operador decidió en última instancia seguir con el negocio como operadora virtual. El número de este tipo de operadores ha crecido mucho los últimos años, debido a su importancia se hablará de ellos más adelante. El periodo de concesión de estas licencias termina el 31 de Diciembre de 2030.

### 3.1.2 Operadoras móviles virtuales (OMV)

Hace unos pocos años han surgido en España como compañías novedosas las operadoras móviles virtuales [11]. Estas empresas son de nueva creación como Yoigo, PepePhone o Eroski o bien son secciones de empresas que ya ofrecen servicios de ADSL y telefonía fija como Jazztel, ONO o Euskaltel. Dichas empresas ofrecen servicios de telefonía, en su mayoría de segunda y tercera generación, pero no tienen red propia desplegada ni son concesionarias de bandas del espectro radioeléctrico. Para prestar los servicios recurren entonces al alquiler de equipamiento perteneciente a las grandes operadoras que ya están asentadas y que poseen grandes redes ya implementadas. El concepto, aunque es nuevo dentro del marco de las comunicaciones móviles ya se venía desarrollando dentro de los servicios de telefonía

fija y ADSL con operadores que ofrecían conexiones a través de los operadores asentados o de concesiones de infraestructura de los gobiernos locales y autonómicos.

Existen diferencias entre las operadoras móviles virtuales a la hora de gestionar sus servicios. Algunas poseen equipos de comunicaciones propios pero se alojan en emplazamientos (torres, edificios...) pertenecientes a otras operadoras y además utilizan canales alquilados de la red troncal de otros operadores para comunicar sus estaciones base. Otras en cambio utilizan exclusivamente canales alquilados y disponen únicamente de equipos de gestión propios para gestionar la información de sus clientes. Las opciones son muy variadas teniendo como variable el grado de integración de una compañía virtual dentro de una con infraestructura propia.

El negocio de las operadoras virtuales contrasta con el de las operadoras establecidas anteriormente debido a que las tarifas ofrecidas son muy diferentes. Si bien es cierto que en el apartado de datos las tarifas planas han desbancado al cobro por volumen y son ofrecidas por ambas, las tarifas planas llamadas de voz no están contempladas en las operadoras móviles para la mayoría de los casos. Por ello, se ofrecen tarifas agresivas bajando el precio por minuto pero a costa de abonar un establecimiento de llamada cada vez que se inicia una comunicación. Debido a que la duración de las llamadas no sobrepasa en la mayoría de los casos un par de minutos, las operadoras móviles virtuales pueden llegar a tarifar el minuto de llamada de voz incluso por debajo del coste que implica para ella el pago a la compañía que le presta su infraestructura.

### 3.2 Legislación del espectro radioeléctrico en España

El espectro radioeléctrico es considerado un bien de dominio público en nuestro país. Según esto, corresponde a la Ley regular los bienes de dominio público y lo realiza mediante la Ley General de Telecomunicaciones (LGT) [12]. La titularidad, la gestión y el control corresponden al Estado. La raíz de esta designación está en la escasez del recurso y en la coordinación internacional por lo que se atribuye a los gobiernos la responsabilidad de controlar el espectro y hacer cumplir una serie de requisitos a los entes privados que deseen prestar sus servicios de telecomunicaciones inalámbricas. La LGT comprende también las atribuciones a los operadores antes mencionados. Además el Estado debe someterse para la asignación de éste bien común a diferentes Tratados Internacionales y a la normativa fijada por la ITU para la clasificación de los servicios facilitando así la interoperabilidad entre redes de diferentes naciones. Todo ello no implica, por otra parte, que el Estado sea libre de regular la competencia y asignar el espectro disponible mediante los procedimientos que considere oportunos.

En el apartado de gestión nos encontramos con que el Estado se convierte en una especie de inspector que debe comprobar las emisiones de cada operador, controlar las interferencias potencialmente perjudiciales y sancionar todas aquellas conductas que se salgan del marco legal fijado por la LGT. Los métodos de control principales para asegurar un uso del espectro radioeléctrico eficiente son la renovación periódica de licencias que permiten el libre mercado y la necesidad del operador solicitante de cumplir una serie de requisitos de calidad en la prestación de sus servicios. El organismo encargado de asignar títulos habilitantes para el uso de las diferentes bandas del espectro licenciadas es la Agencia Estatal de Radiocomunicaciones. En este caso, para cualquier uso y/o tecnología, se diferencian dos usos: sin contenido económico (como los radioaficionados) o la explotación del recurso para negocio (en cuyo caso, el solicitante deberá acreditar la condición de operador). Éste organismo se

encarga también del cobro de la gestión y liquidación de las tasas que cada concesionario deberá abonar por las licencias asignadas.

Una vez explicada la regulación, se comentarán las posibles infracciones y sanciones derivadas del uso indebido del espectro electromagnético. Para los entes privados adjudicatarios de licencias, la violación de las condiciones de la concesión o el impago de las tasas traería consigo la suspensión o pérdida de los derechos adquiridos de ocupación del bien público. Para el caso de utilización sin el correspondiente permiso, se considera una infracción muy grave o grave del reglamento de la LGT. Los infractores por lo tanto, deberán satisfacer el pago de las tasas que hubiera debido abonaren caso de estar disfrutando de un título para la utilización del espectro. A esto se debe añadir un extra por la ocupación de espectro sin licencia. Esto deviene en una relación circular, por lo tanto, el uso de frecuencias licenciadas conlleva el pago de las mismas y a su vez, el impago de las tasas elimina el derecho de explotación de las licencias. La única opción para utilizar alguna de las frecuencias asignadas es mediante contrato con uno de los operadores que poseen alguna licencia en vigor. Corresponde por tanto a las empresas fijar las condiciones, el precio y el tiempo de uso.

### 3.3 Nueva generación de comunicaciones: LTE

Debido a la gran popularidad de las redes móviles terrestres y a las limitaciones de la tecnología UMTS en cuanto a velocidad en la transmisión de datos, se decidió crear un nuevo estándar para las comunicaciones. El principal objetivo del estándar es soportar los nuevos servicios de comunicaciones como el tiempo real, los juegos *online* desde plataformas móviles, *streaming*... que necesitan un gran ancho de banda para funcionar correctamente y que se ven muy limitados por las redes 3G. Para ello y debido al adelanto tecnológico desde las generaciones móviles anteriores, se han buscado nuevas técnicas para utilizar el espectro de forma más eficiente, además de reducir el consumo energético de los terminales. Estas dos características son las más limitantes debido por una parte a la escasez de frecuencias y por otra al límite tecnológico de las baterías, fundamentales cuando se trata de aumentar la movilidad de los dispositivos. Otra característica importante es la creación como red *All-IP* sin recursos dedicados para la voz y transmitiendo la información de la misma forma sea cual sea su naturaleza. Esta tendencia es generalizada dentro de todas las redes de comunicaciones por lo que posibilita la interoperabilidad con otras redes de diferente naturaleza. Además se utilizan los mismos protocolos y niveles lógicos en la red de red (*Internet*) por lo que es mucha más sencillo y eficiente el acceso.

Actualmente los terminales de gama media-alta lanzados al mercado durante el último año ya son compatibles con ésta tecnología. El problema está en la infraestructura de los operadores que no ven viable la inversión. Algunos países ya han subastado el espectro reservado para la tecnología y algunos operadores están realizando pruebas en entornos reducidos. Pese a tener un funcionamiento bastante diferente a los sistemas UMTS, la ITU no reconoce a LTE [13] como la cuarta generación sino como 3,9G y reserva esa denominación para un estándar que aún está en proceso y que se conoce como LTE Advance. Con la aparición de terminales compatibles se descubrió que al no haber acuerdos entre países y no estar claro el futuro de la tecnología, los fabricantes han realizado terminales que pueden no ser compatibles con las redes LTE que se vayan a despegar en determinados países. Y al tratarse de un problema de hardware sería necesario para los usuarios un cambio de terminal.

Está claro que LTE es la evolución lógica de las redes y que supone un aumento de velocidad en las comunicaciones, un uso más eficiente de los recursos energéticos y frecuenciales pero en la actualidad supone una fuerte inversión por parte de los operadores y no parece que estén muy dispuestos a asumirla. El mercado de las comunicaciones móviles siempre ha estado fuertemente marcado por el empuje de los clientes pero parece que con las redes de tercera generación se ha alcanzado el techo y los operadores no tienen claro que sus clientes estén dispuestos a pagar la diferencia en sus tarifas para tener mayor velocidad. De todos modos, se trata de un negocio que cambia rápidamente por lo que en cuanto alguien dé el primer paso, la competencia no tardará en imitarles.



Ilustración 20: Despliegue de tecnología LTE en España por empresa y fecha

No obstante, algunas compañías han empezado a desplegar soluciones mixtas [14] junto con los últimos estándares WiFi. Aunque esta tecnología tiene mucho menos alcance que las tecnologías móviles, poseen un ancho de banda mayor. Uno de los pioneros en ofrecer este tipo de soluciones en España es ONO. El operador utiliza los equipos WiFi de sus abonados a una conexión fija de fibra óptica y los configura de tal forma que radien una red a la que pueden acceder otros abonados de la compañía. Es cierto que el uso por parte de terceros puede ralentizar la conexión del abonado que ofrece su ancho de banda pero la operadora cuenta con velocidades de conexión lo suficientemente altas para que el efecto sea mínimo. De todos modos se trata de una experiencia piloto en las ciudades de Santander y Alicante y aún no se conocen las implicaciones de seguridad y calidad del servicio.

Tras conocer la evolución y el estado actual de las comunicaciones móviles en nuestro país, se comenzará a partir del siguiente capítulo, a describir la parte técnica del presente proyecto.

## Capítulo 4 – Analizador de redes GSM

## 4 Analizador de redes GSM

Aunque existen sistemas completos de captura y análisis de tramas de interfaz radio GSM el precio del equipamiento es elevado. Además los equipos se controlan mediante software privativo que obliga a adquirir licencias de uso que suponen una gran desembolso económico. Estas soluciones son usualmente empleadas por empresas del sector que necesitan toda esa potencialidad, amortizando su coste. Debido a que se trata de conseguir un analizador para un entorno de laboratorio y con un coste moderado, se ha recurrido a software libre. Estos sistemas abiertos cuentan con menor potencial y están más limitados en cuanto a funcionalidades, resultan más eficientes, en términos de vista económicos, dentro de un laboratorio. La contrapartida es que su desarrollo es menos y en la mayoría de los casos la complejidad en el manejo y la instalación es mayor que en los equipos comerciales.

Se ha utilizado como base el proyecto OsmocomBB [15] para implementar un analizador de GSM. Está dotado con las funcionalidades suficientes para nuestro entorno de pruebas.

### 4.1 Proyecto OsmocomBB



El proyecto OsmocomBB es una plataforma de software libre que implementa una serie de librerías para interactuar con los sistemas GSM. Aunque existen sistemas propietarios específicos para dicha función, el proyecto persigue eliminar la necesidad de los mismos e interactuar mediante software con licencia abierta. Los principales objetivos son proporcionar los *drivers* necesarios en un sistema operativo UNIX para poder interactuar con la información contenida en las tramas GSM y presentar ésta de forma sencilla dentro de un interfaz de usuario. Para ello es necesario interpretar dentro de un terminal móvil las capas 1 a 3 de los protocolos GSM utilizando así el terminal como un analizador espectral de las frecuencias utilizadas en GSM como si de un periférico más se tratase. La meta final es crear un software capaz que unido a un teléfono compatible pueda autenticarse en redes GSM y recibir/enviar llamadas, SMS...

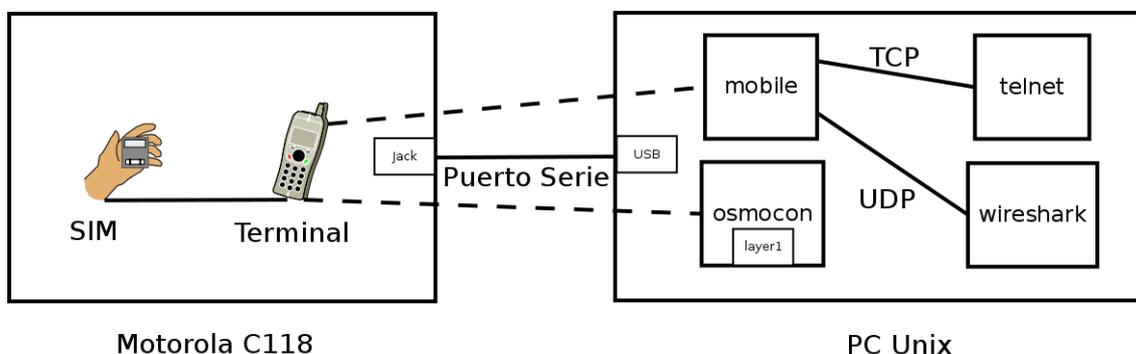


Ilustración 22: Esquema general analizador GSM

El proyecto OsmocomBB se divide en dos partes: una que consiste en el software especialmente diseñado para los terminales móviles compatibles y otro focalizado en el desarrollo de paquetes software desarrollados para sistemas Unix que son capaces de interactuar con las rutinas cargadas en el terminal móvil y que posibilitan el análisis del tráfico capturado por el mismo. El esquema general que se explicará a continuación es el mostrado en la Ilustración 22.

## 4.2 Software para el terminal móvil

Desde el principio del proyecto OsmocomBB, se escogieron como terminales base los modelos CXXX de la marca Motorola. Éstos móviles, además de resultar baratos, están basados en chip de comunicaciones *Calypso* de tipo ARM y que están presentes en multitud de aparatos electrónicos sobre todo en aquellos en los cuales la movilidad y el consumo energético son críticos para su funcionamiento. *Calypso*, además de estar presente en gran variedad de teléfonos móviles GSM, cuenta con diversa documentación de libre acceso sobre su arquitectura a nivel de registros. Sin embargo los modelos mencionados se encuentran actualmente descatalogados por el fabricante y no resulta sencillo adquirirlos.

El procesador digital de señal (DSP) con el que cuentan los terminales, implementa la mayoría del procesamiento de señal GSM, sobretodo en la parte de recepción. Cuenta con API's de acceso libre para su comunicación con el núcleo ARM así como con la memoria RAM presente en los terminales.

El primer paso realizado desde la comunidad OsmocomBB, es la creación de un *driver* capaz de manejar el chip *Calypso* residente en el teléfono e interactuar con el DSP mediante un API sencillo. Así inicialmente se desarrollan las capas 1, 2 y 3 de GSM en el terminal móvil incluyendo interfaces abiertos que permiten interactuar desde equipos externos, es decir, modificar el comportamiento del terminal en la red, controlar la información que se transmite y recibe, etc...

Para generar el *firmware* necesario, que se ejecutará en el teléfono móvil, se habilita un entorno de compilación cruzada para ARM. Osmocom ofrece varios *firmware* específicos para los terminales compatibles, pero en nuestro caso sólo utilizaremos uno de ellos llamado *layer1* que nos permite, con ayuda de otros programas para el PC, enviar las tramas capturas por el terminal para su análisis. También se ha empleado el *firmware rssi* que permite observar en la pantalla gráficas del nivel de señal recibido en cada canal frecuencial.

Existen diferentes fórmulas para cargar los *firmware* dentro del terminal. Por un lado se tiene la opción de reemplazar completamente el *firmware* del teléfono sobrescribiendo en su memoria *flash* pero, en este caso el terminal queda inutilizado para operar como teléfono móvil GSM. Otra opción, más recomendada para entornos de evaluación como el que se emplea en este proyecto, facilita la carga directamente en la memoria RAM del dispositivo por lo que permite volver al estado original al reiniciar el dispositivo.

Para la carga del *firmware* se utiliza un programa para PC Unix llamado *osmocon*, que a la vez sirve de interfaz entre el terminal y las aplicaciones de gestión externas. La conexión entre el terminal móvil y el dispositivo de control se establece a través de un canal serie. La conexión física se realiza desde un conector *jack* compartido con el puerto de audio en el teléfono y un puerto USB del PC.

### 4.3 Software para el PC

Una vez que se ha instalado el *firmware* dentro del terminal móvil, es hora de ejecutar en el PC el programa necesario para interactuar con él. Para nuestro objetivo, la rutina a cargar es la denominada *mobile*. Se trata de un programa que permite manejar el terminal y que contiene las capas 2 y 3 de GSM que junto con la capa 1 ya instalada en el móvil mediante el *firmware layer1* posibilita la autenticación del móvil en la red así como realización de llamadas de voz y el envío de SMS. También es posible realizar otros procedimientos como la actualización de posición y los mecanismos de encriptación GSM.

```

=>FB @ FNR 704339 fn_offset=704339 qbits=4836
Synchronize_TDMA
LOST 3717!
SB1 (1408685:1): TOA= 26, Power=-90dBm, Angle= 438Hz
=> SB 0x00ae0995: BSIC=37 fn=704351(531/11/41) qbits=12
Synchronize_TDMA
=>FB @ FNR 1408684 fn_offset=704351 qbits=4920
LOST 1907!
L1CTL_RESET_REQ: FULL!L1CTL_FBSB_REQ (arfcn=555, flags=0x7)
Starting FCH RecognitionFB0 (704375:2): TOA= 1296, Power= -8
9dBm, Angle= 4080Hz
FB1 (704385:8): TOA= 8779, Power= -90dBm, Angle= 634Hz
fn_offset=704384 (fn=704385 + attempt=8 + ntdma = 7)
delay=9 (fn_offset=704384 + 11 - fn=704385 - 1
scheduling next FB/SB detection task with delay 9
=>FB @ FNR 704383 fn_offset=704383 qbits=4932
Synchronize_TDMA
LOST 1878!
SB1 (1408774:1): TOA= 47, Power= -89dBm, Angle= 470Hz
=> SB 0x01358a76: BSIC=29 fn=1724749(1300/13/31) qbits=96
Synchronize_TDMA
=>FB @ FNR 1408773 fn_offset=1724750 qbits=4
LOST 1939!
r updated.
<0004> gsm322.c:4663 Read from neighbour cell 19 (rxlev -81).
<0004> gsm322.c:4571 Syncing to new neighbour cell 12.
<0003> gsm322.c:469 Sync to ARFCN=12 rxlev=-110 (No sysinfo yet, ccch m
ode NONE)
<0003> gsm322.c:2938 Channel synched. (ARFCN=12, snr=14, BSIC=37)
<0001> gsm322.c:2959 using DSC of 90
<0004> gsm322.c:4642 Synced to neighbour cell 12.
<0003> gsm322.c:692 Starting CS timer with 2 seconds.
<0003> gsm48_rr.c:4816 Channel provides data.
<0001> gsm48_rr.c:1961 New SYSTEM INFORMATION 4 (mcc 214 mnc 07 lac 0x0f4
2)
<0003> gsm322.c:702 stopping pending CS timer.
<0003> gsm322.c:2568 Relevant sysinfo of neighbour cell is now received o
r updated.
<0004> gsm322.c:4663 Read from neighbour cell 12 (rxlev -110).
<0004> gsm322.c:4571 Syncing to new neighbour cell 555(DCS).
<0003> gsm322.c:469 Sync to ARFCN=555(DCS) rxlev=-92 (No sysinfo yet, cc
h mode NONE)
<0003> gsm322.c:2938 Channel synched. (ARFCN=555(DCS), snr=16, BSIC=29)
<0001> gsm322.c:2959 using DSC of 90
<0004> gsm322.c:4642 Synced to neighbour cell 555.
<0003> gsm322.c:692 Starting CS timer with 2 seconds.

```

Ilustración 23: Terminales de salida de datos, osmocom a la izquierda y mobile a la derecha

Cuando se realiza la ejecución ambos programas (*mobile* y *osmocon*) se observa en el terminal que la sincronización con el terminal se ha completado con éxito. A partir de este punto se puede acceder al menú de configuración mediante *telnet* a un servidor de comando ejecutado por el programa *mobile*. Los comandos ejecutados serán traducidos por el programa y se enviarán al móvil así como las respuestas que este envía a su vez. Pueden observarse multitud de parámetros de la red GSM a la que se encuentra conectado el móvil así como medidas realizadas por el terminal de las redes vecinas. Además se puede acceder a los servicios propios de estándar GSM e iniciar, por ejemplo, una llamada de voz o enviar un SMS. Previo a la ejecución se puede seleccionar, bien como parámetro o mediante el fichero de configuración, el nivel de información mostrada en el terminal de los datos capturados por el terminal aunque también pueden ser configurados mediante comandos.

Además, el software decodifica los datos que captura el móvil por lo que es posible observar todas y cada una de las medidas y comprobaciones que realiza el móvil en tiempo real. La consola de ejecución mostrará en todo momento (Ilustración 23) los procedimientos que está llevando a cabo el terminal como medidas de potencias de las estaciones base más cercanas, autenticaciones, comprobaciones de la SIM, sincronización...

Si observamos el flujo de datos de la Ilustración 24, el procedimiento de captación comienza en el terminal móvil con el *firmware* adecuado cargado en su RAM y en ejecución. La señal es captada por la antena y transformada a banda base por el mezclador incluido en el terminal. Esto genera una señal, aún analógica en modulación I/Q que es transformado por otro chip, también incluido en los terminales Motorola a modulación I/Q pero en este caso digital que entra por el puerto al chip Calypso por su puerto serie de banda base.

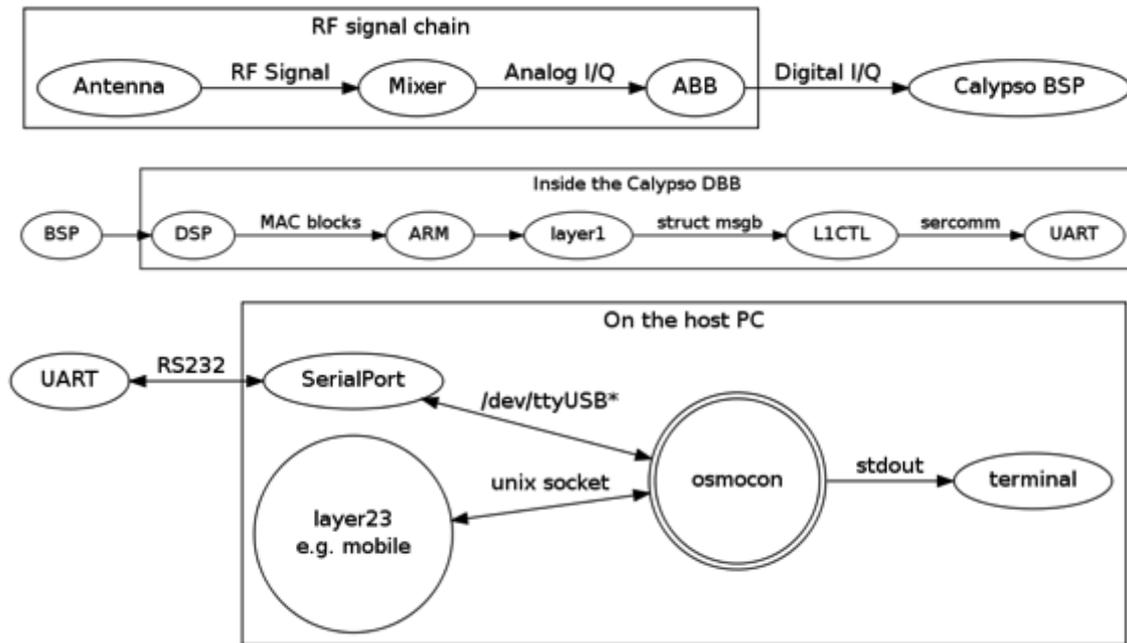


Ilustración 24: Esquema de funciones dentro de cada elemento

Una vez digitalizadas, las muestras son enviadas al DSP del teléfono móvil donde son decodificadas, demoduladas, se elimina su entrelazado y se procesan antes de enviarse a la CPU del procesador ARM. Dentro de la CPU es donde comienza a operar el *firmware* customizado, *layer1*, que se ha introducido previamente en la RAM. Por último los datos llegan a la UART que gestiona la conexión entre el terminal y el PC a través del puerto serie hasta el puerto USB. A partir de éste momento los datos son gestionados por el PC mediante el programa *mobile*.

### 4.4 Integración con analizador de protocolos (GSMTAP)

Hasta ahora se ha mostrado las opciones de las que se dispone para controlar el móvil y capturar datos referentes a la red GSM. Pero además, al disponer en tiempo real a través del puerto serie de la información que recoge el móvil sobre la red, estos datos pueden exportarse a otro programas para realizar un análisis más exhaustivo.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR)	Paging Request Type 1
2	0.017964	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR)	Immediate Assignment
3	0.045964	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR)	Paging Request Type 1
4	0.064029	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR)	Paging Request Type 1
5	0.092041	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR)	Paging Request Type 1
6	0.111106	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR)	Immediate Assignment
7	0.138413	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR)	Paging Request Type 1

```

Frame 24: 81 bytes on wire (648 bits), 81 bytes captured (648 bits)
Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
Internet Protocol Version 4, Src: 127.0.0.1 (127.0.0.1), Dst: 127.0.0.1 (127.0.0.1)
User Datagram Protocol, Src Port: 52847 (52847), Dst Port: gsmtap (4729)
GSM TAP Header, ARFCN: 989 (Downlink), TS: 0, Channel: PCH (0)
  Version: 2
  Header length: 16 bytes
  Payload Type: GSM Um (MS<->BTS) (1)
  Time Slot: 0
  ..00 0011 1101 1101 = ARFCN: 989
  .0. .... .... = UpLink: 0
  Signal/Noise Ratio (dB): 190
0000 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00 .....E
0010 00 43 b0 20 40 00 40 11 8c 87 7f 00 00 01 7f 00 .....C.@.@.
0020 00 01 c8 6f 12 79 00 2f fe 42 02 04 01 00 03 dd .....0.y/.B
0030 0a 00 00 0c e9 f0 05 00 00 00 15 09 21 00 01 f0 .....
0040 2b .....
    
```

Ilustración 25: Software de análisis de protocolos Wireshark

Con el fin de facilitar la visualización e interpretación de las diferentes tramas temporales que conforman el estándar GSM, es posible además exportar los datos en hacia el analizador de protocolos de licencia libre WireShark [16] en tiempo real. Esta opción se consigue arrancando el programa desde la consola e introduciendo los parámetros necesarios para que se redirija la interfaz por la que entran los datos hacia el analizador. El propio software interpreta las tramas GSM recogidas por el analizador gracias a un disector de protocolos para WireShark llamado GSMTAP [17].

GSMTAP incorpora una pseudo-cabecera que habilita la transferencia y el análisis de las tramas del interfaz Um del estándar GSM por parte del analizador WireShark. Este muestra las tramas encapsularlas dentro de paquetes UDP/IP utilizados en la inmensa mayoría de las redes de comunicaciones actuales. De esta manera, se consigue que el analizador de protocolos interprete de forma correcta las tramas *broadcast* que envía la estación base hacia los terminales que campean en la celda y que son capturadas por nuestro analizador. Los campos que añade la cabecera, que no incluyen el *payload* que realmente se transmite en GSM, son los mostrados en la Tabla 4.

Campo	Longitud	Descripción
versión	8 bits	Versión del protocolo GSMTAP
longitud	8 bits	Longitud de la cabecera GSMTAP en palabras de 32 bits
tipo	8 bits	Tipo de trama GSMTAP
timeslot	8 bits	Timeslot dentro de la trama GSM
arfcn	16 bits	Canal de frecuencia que transporta la trama
nivel de señal	8 bits	Nivel de recepción de señal en dBm
snr	8 bits	Nivel señal/ruido en dB
número de trama	32 bits	Número de trama de la secuencia de GSM
tipo de canal GSM	8 bits	Tipo de canal/ráfaga GSM
antena	8 bits	Número de antena
sub slot	8 bits	Subslot dentro del timeslot de la trama GSM
reservado	8 bits	Reservado para uso futuro

Tabla 4: Elementos cabecera GSMTAP

Dicha cabecera se conforma mediante información recogida por el terminal en las tramas FCCH de sincronización en frecuencia y SCH. Los datos anteriores son añadidos por el programa *mobile* a las tramas GSM capturadas por el terminal y enviados como datos IP al analizador WireShark. Este conoce el protocolo y es capaz de descomponer las tramas para facilitar su análisis.

Cabe destacar que las tramas de tráfico específico para el terminal que está realizando la captura, tanto como para el enlace descendente como para el ascendente, se muestran encapsuladas en el protocolo LAPD heredado de las redes antiguas RDSI. El motivo es, como se comentó anteriormente, reutilizar protocolos existentes tanto para el analizador de protocolos. WireShark cuenta con el disector de protocolo y es capaz de interpretar las tramas directamente. Al tratarse de comunicación punto a punto también incorporan en este caso la cabecera descrita en la Tabla 4.

## 4.5 Manejo y obtención de resultados

A continuación se describe el procedimiento seguido para la captura y análisis del tráfico originado en una red GSM mediante las herramientas proporcionadas desde el proyecto OsmocomBB. Una vez realizada la configuración mencionada en las secciones anteriores, podemos ejecutar determinados procedimientos de análisis para conocer características de la red en la que el terminal de análisis se encuentra conectado. Se observarán parámetros no sólo de la configuración de la red sino que también se podrá conocer el estado de la misma en tiempo real.

### 4.5.1 Arranque del analizador

En primer lugar debe establecerse el canal de comunicaciones entre el terminal móvil C118 de Motorola y el equipo de control. Para ello el terminal móvil habilita un puerto serie que unido a las capacidades del *firmware layer1* envía la información capturada hacia el PC. El teléfono debe llevar instalada una tarjeta SIM válida para la red que queremos monitorizar o no se obtendrá la información completa.

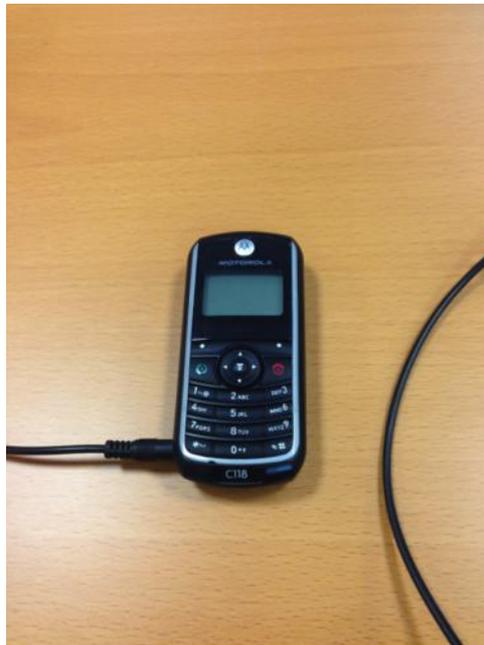


Ilustración 26: Conexión del terminal con el PC

El siguiente paso es ejecutar el programa *mobile* en del PC de forma que el tráfico capturado por el teléfono pueda ser enviado e interpretado a la consola Linux. Además se permite acceder mediante terminal a una consola donde se puede interactuar con el terminal de captura para obtener información más precisa.

```
/opt/osmocom-bb/src/host/layer23/src/mobile$ sudo ./mobile -i  
127.0.0.1
```

Se observa que abre contra el interfaz de *loopback* del PC para poder acceder al terminal remoto dentro del mismo equipo. Tras la ejecución del comando nos indicará que ya está accesible la consola en el puerto 4247 pero que no detecta la estación móvil de captura. Se ejecutará:

```
/opt/osmocom-bb/src/host/osmocon$ sudo ./osmocon -p /dev/ttyUSB0  
-m c123xor  
../../../../target/firmware/board/compal_e88/layer1.compalram.bin
```

Mediante el siguiente comando cargamos el programa en la RAM del terminal Motorola. Como se observa debe especificarse el interfaz de conexión, que en nuestro caso será el puerto serie habilitado a través del USB. Además es necesario definir la familia del modelo de terminal (*c123xor*) y el *firmware* que se desea introducir en el terminal. Para capturar tramas del protocolo se necesita el *firmware layer1*. De entre todos los disponibles se emplea el tipo *compalram* que son los específicos para ser cargados en memoria RAM del terminal sin necesidad de instalarse. De esta manera evitamos escribir la memoria *flash* del terminal posibilitando así que tras un reinicio éste siga funcionando como terminal móvil corriente. Se recomienda la ejecución de cada programa en una consola diferente debido a que ambas muestran un *log* con las lecturas de datos y los procesos que están llevando a cabo.

Ahora veremos cómo clasificar la información y acceder a ella de forma que pueda ser analizada. Se han realizado las pruebas con dos tarjetas SIM para obtener mayor información. Por una parte se ha utilizado una SIM convencional del operador Movistar y por otro, una SIM personalizada. Estas tarjetas pueden programarse mediante un lector/escritor de tarjetas inteligentes [18] pero para este proyecto se ha utilizado la configuración que tenían almacenada por defecto.

#### 4.5.2 Obtener información mediante terminal

El primer modo de acceso a la información sobre la estación base y el terminal que nos ofrece nuestro analizador, es abriendo una consola remota contra el puerto 4247 del equipo donde se ejecuta. Es posible modificar el puerto pero tiene ese configurado por defecto. Este es el interfaz habilitado en *mobile* para poder modificar el comportamiento del terminal móvil bajo su control. Podremos cambiar la configuración del programa, mostrar datos relevantes de los equipos y protocolos analizados y acceder a algunos de los servicios ofrecidos por las redes GSM. Accedemos a la consola introduciendo el siguiente comando:

```
/path$ telnet localhost 4247
```

Por simplicidad, el primer comando a introducir es *enable*. De ésta forma tenemos acceso a todos los parámetros y configuraciones disponibles. Es recomendable familiarizarse con las opciones antes de utilizar el acceso completo debido a que puede dañarse la tarjeta SIM o desestabilizar la red a la que nos conectamos.

##### 4.5.2.1 Información acerca de la estación móvil

Aunque la misión principal del analizador es obtener información relevante acerca de la red, también resulta interesante conocer los parámetro de configuración del terminal y más concretamente, de la SIM que hemos introducido. Como puede comprobarse en la Ilustración 27 y en la Ilustración 28, mediante el comando *show subscriber* obtenemos las siguientes capturas según la tarjeta presente en el terminal.

```
OsmocomBB> show subscriber 1
Mobile Subscriber of MS '1':
IMSI: 460003113237934
ICCID: 8986008219031386052
Service Provider Name: OpenBTS
SMS Service Center Address: 00345555
Status: U1_UPDATED IMSI attached TSMI 0x5ffd95ba
      LAI: MCC 214 MNC 29 LAC 0x1f41 (Spain, 29)
Registered PLMN: MCC 214 MNC 29 (Spain, 29)
Access barred cells: no
Access classes: C0 C1 C2 C3 C4 C5 C6 C7 C8 C9 C10 C11 C12 C13 C14 C15
List of preferred PLMNs:
  MCC  |MNC
  -----+-----
    214 |29      (Spain, 29)
List of forbidden PLMNs:
  MCC  |MNC  |cause
  -----+-----
    214 |04   |#255      (Spain, Yoigo)
```

Ilustración 27: Captura de datos con SIM personalizada

```
OsmocomBB# show subscriber 1
Mobile Subscriber of MS '1':
IMSI: 214075531908988
ICCID: 8934075100214963076
SMS Service Center Address: +34609090909
Status: U1_UPDATED IMSI attached TSMI 0x6c0d7625
      LAI: MCC 214 MNC 07 LAC 0x0f42 (Spain, movistar)
Key: sequence 0 72 c0 c6 66 c5 f9 1c 82
Registered PLMN: MCC 214 MNC 07 (Spain, movistar)
Access barred cells: no
Access classes: C8
List of preferred PLMNs:
  MCC  |MNC
  -----+-----
    208 |01      (France, Orange)
    208 |20      (France, Bouygues)
    234 |10      (Guernsey, O2)
    268 |06      (Portugal, TMN)
    268 |03      (Portugal, Optimus)
    222 |01      (Italy, TIM)
    262 |07      (Germany, O2)
    204 |08      (Netherlands, KPN)
    604 |00      (Morocco, Moditel)
    232 |03      (Austria, T-Mobile)
    228 |02      (Switzerland, Sunrise)
    272 |02      (Ireland, O2)
    334 |030     (Mexico, 030)
    202 |10      (Greece, Wind)
    226 |10      (Romania, Orange)
    226 |03      (Romania, Cosmote)
```

Ilustración 28: Captura de datos con SIM del operador Movistar

Lo primero que observamos en las capturas, es que el terminal está asociado con la red del operador *Movistar*. Además aparecen los parámetros IMSI, ICCID así como la lista preconfigurada de redes preferidas y prohibidas de la tarjeta SIM. La tarjeta SIM contiene estos datos en una estructura descrita en el estándar GSM 11.11 [19] para asegurar la interoperabilidad. Observamos que está asociada a la red y que se le ha asignado un TSMI dentro de la misma. También se especifican todos los parámetros de la red a la que se encuentra conectado. En los dos ejemplos puede comprobarse que diferentes tarjetas pueden contener diferentes configuraciones. Se observa por ejemplo que varía el número de redes preferidas y prohibidas.

#### 4.5.2.2 Información sobre celdas GSM

Es posible mediante el comando *show cell* obtener información sobre la estación base a que se encuentra conectado el terminal. Se observa en las capturas de la Ilustración 29 y la Ilustración 30 los parámetros de configuración de la celda así como datos relativos a la intensidad de la señal y el ruido que recibe el móvil desde la antena GSM. Se puede apreciar que en la Ilustración 29 una sola red debido a que las redes de los operadores comerciales no se encuentran entre las predeterminadas por la tarjeta SIM. En la captura utilizando la SIM del operador Movistar (Ilustración 30) se pueden observar varias antenas adyacentes y las mediciones que se realizan de cada una de ellas.

```
OsmocomBB> show cell 1
ARFCN | MCC | MNC | LAC | cell ID | forb.LA | prio | min-db | max-pwr | rx-lev
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----
770DCS | 214 | 29 | 0x1f41 | 0x01a9 | no | normal | -110 | 7 | -52
```

Ilustración 29: Redes disponibles para la SIM personalizada

```
OsmocomBB# show cell 1
ARFCN | MCC | MNC | LAC | cell ID | forb.LA | prio | min-db | max-pwr | rx-lev
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----
3 | 214 | 07 | 0x0f42 | 0x0413 | n/a | n/a | -102 | 5 | -96
6 | 214 | 07 | 0x0f42 | 0x003f | n/a | n/a | -102 | 5 | -95
12 | 214 | 07 | 0x0f42 | 0x0962 | n/a | n/a | -102 | 5 | <=-110
16 | 214 | 07 | 0x0f42 | 0x0412 | n/a | n/a | -102 | 5 | -98
17 | 214 | 07 | 0x0f42 | 0x0963 | n/a | n/a | -102 | 5 | -96
19 | 214 | 07 | 0x0f42 | 0x0961 | no | normal | -102 | 5 | -76
525DCS | n/a | n/a
542DCS | 214 | 07 | 0x0f42 | 0x0aff | n/a | n/a | -102 | 0 | -97
555DCS | 214 | 07 | 0x0f42 | 0x0964 | n/a | n/a | -102 | 0 | -75
```

Ilustración 30: Redes disponibles para SIM del operador Movistar

Las capturas presentan no solo la medida de señal sino también la información relativa a las redes a las que se tiene acceso. Cada operador distribuye sus frecuencias disponibles espacialmente por lo que se observan varios canales a los que el terminal puede conectarse. El terminal se conectará a la frecuencia que le ofrezca un mayor nivel de señal y realizará revisiones periódicas para determinar cuál de ellas es la adecuada.

Band	Name	ARFCN	Uplink (MHz)	Downlink (MHz)
GSM400	GSM450	$259 \leq n \leq 293$	$450.6 + 0.2 \times (n - 259)$	$f_{up}(n) + 10$
	GSM480	$306 \leq n \leq 340$	$479.0 + 0.2 \times (n - 306)$	$f_{up}(n) + 10$
GSM700	GSM750	$438 \leq n \leq 511$	$747.2 + 0.2 \times (n - 438)$	$f_{up}(n) + 30$
GSM850	GSM850	$128 \leq n \leq 251$	$824.2 + 0.2 \times (n - 128)$	$f_{up}(n) + 45$
GSM900	Primary GSM	$1 \leq n \leq 124$	$890 + 0.2 \times n$	$f_{up}(n) + 45$
	Extended GSM	$0 \leq n \leq 124$	$890 + 0.2 \times n$	$f_{up}(n) + 45$
		$975 \leq n \leq 1023$	$890 + 0.2 \times (n - 1024)$	
GSM Rail	$0 \leq n \leq 124$ $955 \leq n \leq 1023$	$890 + 0.2 \times n$ $890 + 0.2 \times (n - 1024)$	$f_{up}(n) + 45$	
GSM1800	GSM1800 (DCS1800)	$512 \leq n \leq 885$	$1710.2 + 0.2 \times (n - 512)$	$f_{up}(n) + 95$
GSM1900	GSM1900 (PCS1900)	$512 \leq n \leq 810$	$1850.2 + 0.2 \times (n - 512)$	$f_{up}(n) + 80$

Tabla 5: Correspondencia ARFCN con frecuencia principal

El número ARFCN corresponde al identificador de canal. Este se corresponde con la frecuencia principal de emisión de la antena, según el tipo de banda GSM, como indica Tabla 5.

El parámetro LAC es un identificador de las estaciones base según su emplazamiento. Al encontrarse todas cercanas entre sí, se observa que es idéntico para todas las pertenecientes al mismo operador. A su vez, el parámetro *cell ID* corresponde al número identificativo de la antena que radia la red. Los valores *min-db*, *max-power* y *rx-lev* son el nivel de señal a ruido mínimo, la potencia de transmisión máxima y el nivel de señal de recepción respectivamente.

Además, se puede obtener también información sobre las celdas vecinas que detecta el terminal. Introduciendo el comando *show neighbour-cells* se mostrarán los parámetros de las celdas adyacentes.

```
OsmocomBB# show neighbour-cells 1
Serving cell:
ARFCN=555(DCS) RLA_C=-77 C1=25 C2=25 LAC=0x0f42

Neighbour cells:
# | ARFCN | RLA_C | C1 | C2 | CRH | prio | LAC | cell ID | usable | state
-----|-----|-----|----|----|----|-----|-----|-----|-----|-----
1 | 19 | -80 | 23 | 23 | 0 | normal | 0x0f42 | 0x0961 | yes | SYSINFO
2 last | 525 | -82 | 19 | 19 | 0 | normal | 0x0f42 | 0x0965 | yes | SYSINFO
3 | 17 | -88 | 14 | 14 | 0 | normal | 0x0f42 | 0x0000 | yes | SYSINFO
4 | 12 | -93 | 7 | 7 | 0 | normal | 0x0f42 | 0x0962 | yes | SYSINFO
5 | 10 | -94 | - | - | - | - | - | - | no | no sync
6 | 16 | -96 | - | - | - | - | - | - | no | no sync
--- unmonitored cells: ---
7 | 542 | -101 | 8 | 8 | 0 | normal | 0x0f42 | 0x0aff | yes | SYSINFO
8 | 527 | -105 | - | - | - | - | - | - | no | RLA_C
9 | 544 | -106 | - | - | - | - | - | - | no | RLA_C
10 | 531 | -107 | - | - | - | - | - | - | no | RLA_C
11 | 547 | -106 | - | - | - | - | - | - | no | RLA_C
12 | 553 | -105 | - | - | - | - | - | - | no | RLA_C
13 | 532 | -107 | - | - | - | - | - | - | no | RLA_C
```

Ilustración 31: Información sobre celdas vecinas

Existen dos tipos de redes en la captura de la Ilustración 31. Por una parte se encuentran las celdas candidatas a dar servicio al terminal. Es decir, aquellas que se encuentran en monitorización porque pueden ser elegidas por el terminal para conectarse a ellas. El móvil se mantiene observando las redes vecinas para comprobar si reúnen mejores condiciones que la actual para conectarse a ellas. Las otras redes son simplemente ignoradas en el proceso de selección ya que no cumplen los requisitos necesarios. Los requisitos pueden ser estáticos o dinámicos:

- Estáticos: La configuración de la SIM tiene prohibida la conexión a esas redes debido principalmente a que son de un operador de la competencia.
- Dinámicos: Aprovechando las mediciones que realiza el terminal de forma constante, pueden descartarse redes a priori seleccionables debido a que la cobertura o la calidad de la señal no permiten la suficiente calidad de servicio.

Se puede observar mediante el comando *monitor network* (Ilustración 32) la selección de celdas candidatas en tiempo real.

Los parámetros RLA\_C, C1 y C2 son magnitudes calculadas a partir de los parámetros de señal que recibe el terminal. Son específicos para la elección de la celda base a la que el móvil se conecta. El parámetro LAC es un identificador de las estaciones base según su emplazamiento. Al encontrarse todas cercanas entre sí, se observa que es idéntico para todas las pertenecientes al mismo operador. Se puede

observar en la captura superior que la celda con ARFCN=19 que debido a un incremento en el porcentaje de errores o BER el parámetro RLA\_C aumenta haciendo que ése canal ya no sea el más adecuado. Inmediatamente es detectado por el terminal que debe elegir una celda nueva. En este caso se decanta por la celda con ARFCN=17 ya que es, de entre las adecuadas, la más cercana a la frecuencia anterior y por tanto se puede realizar un cambio más rápido.

```
OsmocomBB> monitor network 1
OsmocomBB> % MON: f=19 lev=-77 snr= 0 ber= 22 LAI=214 07 0f42 ID=0961
% MON: cell ARFCN LAC C1 C2 CRH RLA_C bargraph
% MON: serving 19 0x0f42 26 26 -76 =====
% MON: nb 1 555(DCS) -82 =====
% MON: nb 2 17 0x0f42 18 18 0 -84 =====
% MON: nb 3 3 0x0f42 17 17 0 -85 =====
% MON: nb 4 12 0x0f42 11 11 0 -91 =====
% MON: nb 5 525(DCS) -91 =====
% MON: nb 6 10 0x0f42 8 8 0 -94 =====
% MON: f=19 lev=-81 snr= 0 ber= 67 LAI=214 07 0f42 ID=0961
% MON: f=19 lev=-82 snr= 0 ber= 34 LAI=214 07 0f42 ID=0961
% MON: f=19 lev=-92 snr=11 ber=114 LAI=214 07 0f42 ID=0961
% MON: f=19 lev=-94 snr= 1 ber=143 LAI=214 07 0f42 ID=0961
% MON: cell ARFCN LAC C1 C2 CRH RLA_C bargraph
% MON: serving 19 0x0f42 16 16 -86 =====
% MON: nb 1 555(DCS) -85 =====
% MON: nb 2 17 0x0f42 17 17 0 -85 =====
% MON: nb 3 3 0x0f42 17 17 0 -85 =====
% MON: nb 4 525(DCS) -90 =====
% MON: nb 5 12 0x0f42 10 10 0 -92 =====
% MON: nb 6 10 0x0f42 10 10 0 -92 =====
% MON: trigger cell re-selection: better cell

% (MS 1)
% Searching network...
% MON: cell selected ARFCN=17 MCC=214 MNC=07 LAC=0x0f42 cellid=0x0963 (Spain movistar)
```

Ilustración 32: Parámetros de reelección de celda

Por último encontramos el comando *show ba* que permite conocer todas las bandas ocupadas dentro del espectro GSM y que son detectadas por el terminal. Además indica el operador que gestiona dicha frecuencia. Ésta característica, así como la anterior sólo se muestra para aquellas redes que son reconocidas por la tarjeta SIM (Ilustración 33). Por tanto, la tarjeta SIM personalizada no detecta ninguna red ya que no ha sido configurada con ninguna de las redes que se encuentran presentes en nuestro país.

```
OsmocomBB# show ba
% (MS 1)
% On Network, normal service: Spain, movistar
1
Band Allocation of network: MCC 214 MNC 29 (Spain, 29)
514(DCS)
Band Allocation of network: MCC 214 MNC 03 (Spain, Orange)
788(DCS) 789(DCS) 792(DCS) 794(DCS) 797(DCS) 800(DCS) 803(DCS) 805(DCS) 810(DCS) 811(DCS) 813(DCS)
815(DCS) 817(DCS) 877(DCS) 879(DCS) 975 978 981 985 987 989 991
Band Allocation of network: MCC 214 MNC 07 (Spain, movistar)
4 5 10 12 17 18 19 20 516(DCS) 525(DCS) 527(DCS) 531(DCS) 542(DCS) 544(DCS) 547(DCS) 553(DCS) 555(DCS) 557(DCS) 594(DCS)
Band Allocation of network: MCC 214 MNC 01 (Spain, Vodafone)
70 72 74 76 77 79 80 81 83 84 85 87 89 92 93 99 101 120 121 672(DCS) 674(DCS) 675(DCS) 678(DCS)
693(DCS) 704(DCS) 706(DCS)
Band Allocation of network: MCC 214 MNC 04 (Spain, Voigo)
714(DCS) 726(DCS) 727(DCS) 734(DCS) 736(DCS) 737(DCS) 738(DCS) 742(DCS) 743(DCS) 744(DCS) 745(DCS)
746(DCS) 747(DCS) 748(DCS) 751(DCS) 752(DCS) 758(DCS)
```

Ilustración 33: Canales y operadores de las celdas adyacentes

Como se ha podido comprobar, existe una fuerte dependencia con la información contenida en la tarjeta SIM del operador. Aunque en todos los casos es el terminal

quien realiza las medidas, los parámetros contenidos en la SIM permiten conocer las redes que deben ser monitorizadas y cuáles deben ignorarse.

### 4.5.3 Operaciones SIM mediante terminal

Además de mostrar información relevante sobre las redes GSM disponibles, la actual y el terminal móvil, la consola permite realizar configuraciones en ciertos parámetros de la tarjeta SIM. Podremos forzar al terminal que se asocie o que pierda la conexión con la estación base mediante *sim testcard*, *sim reader* y *sim remove*. Como la tarjeta se autentica por defecto, es necesario realizar primero la desconexión. Tras esto podremos comprobar que la información que se ha mostrado anteriormente ya no es accesible. Esto se debe a que ya que la tarjeta SIM ya no está autorizada en ninguna red. No podrá recibir las tramas de información de la estación base y por tanto capturar la información para enviarla al PC Linux.

En el caso de que la tarjeta utilizada tenga activado el código PIN es necesario introducirlo mediante el comando *sim pin XXXX* para tener acceso a los servicios de la tarjeta. De todos modos si sería posible obtener información sobre la red GSM debido a que se trata de un proceso pasivo que realiza el terminal para conocer su entorno y no está bloqueado. Además también puede modificarse el PIN, activarse, desactivarse o desbloquear con los comandos *sim change-pin*, *sim enable-pin*, *sim disable-pin* y *sim unblock-pin* respectivamente.

También es posible realizar una selección manual operador de red. El resultado dependerá de si la tarjeta SIM tiene autorización para entrar en la red seleccionada. Los comandos son los siguientes:

- *network search*: indica al terminal que proceda a la búsqueda de los operadores disponibles.
- *network show*: muestras los operadores de red disponibles.
- *network select*: permite seleccionar, de entre los candidatos, el operador deseado.

Tanto esta opción como las operaciones con el código PIN son características que implementan los propios terminales móviles. Debido a que nos encontramos corriendo un sistema personalizado dentro del terminal, es necesario realizar las operaciones mediante los comandos indicados al no contar con una interfaz gráfica como en el caso de los sistemas móviles convencionales.

Por último el terminal también permite el envío de SMS y la realización de llamadas mediante los comandos *sms* y *call* seguidos del número a marcar. Como en el caso anterior, aunque estos servicios ya están implementados en los terminales estándar, es posible obtener información adicional en el analizador obteniendo los paquetes desde el propio terminal. Como se verá a continuación, es interesante poder realizar los procedimientos anteriores desde el móvil para poder analizarlos con WireShark.

### 4.5.4 Análisis con WireShark

Para exportar las tramas en tiempo real al software de análisis debemos introducir el siguiente comando:

```
$ nc -u -l -p 4729 > /dev/null & wireshark -k -i lo -f 'port
4729'
```

Gracias a la interfaz UDP presente en el programa *mobile*, es posible exportar el tráfico capturado en tiempo real. Para ello contamos con el programa *nc* o *netcat* presente en la gran mayoría de distribuciones Linux y que permite redirigir el flujo entre diferentes programas. La opción *-u* indica que se utilice el protocolo de transporte UDP, *-l* sirve para permanecer en modo de escucha y *-p* asigna el puerto 4729 a la conexión. La salida se redirige a un directorio vacío para WireShark recoja la información recibida por ese puerto desde la IP local del equipo.

Antes de analizar procedimientos para el control de la comunicación definidos en GSM mediante el software de análisis de protocolos WireShark veremos algunas de las tramas que envía la estación base con información acerca de sus parámetros y los parámetros de las redes contiguas. Posteriormente se mostrará el intercambio de tramas que ocurre al realizar determinados procedimientos del estándar GSM.

```

▶ Internet Protocol Version 4, Src: 127.0.0.1 (127.0.0.1), Dst: 127.0.0.1 (127.0.0.1)
▶ User Datagram Protocol, Src Port: 52847 (52847), Dst Port: gsmtap (4729)
▼ GSM TAP Header, ARFCN: 989 (Downlink), TS: 0, Channel: PCH (0)
  Version: 2
  Header length: 16 bytes
  Payload Type: GSM Um (MS<->BTS) (1)
  Time Slot: 0
  ..00 0011 1101 1101 = ARFCN: 989
  .0.. .... .... .... = Uplink: 0
  Signal/Noise Ratio (dB): 190
  Signal Level (dBm): 0
  GSM Frame Number: 846204
  Channel Type: PCH (5)
  Antenna Number: 0
  Sub-Slot: 0
▶ GSM CCCH - Paging Request Type 1

```

**Ilustración 34: Encapsulado de trama en WireShark**

Antes de proceder con los diferentes intercambios en la Ilustración 34 se puede observar cómo se presenta la información en Wireshark. En la captura, cada una de las tramas se encapsula a nivel de aplicación por el protocolo GSMTAP detallado en el apartado 4.3. Los paquetes que Wireshark presenta son el resultado de la redirección de las capturas realizadas internamente por *mobile* y de ahí que estén encapsulados en paquetes. Para la capa de transporte se utiliza UDP entre un puerto libre del PC y el puerto 4729, configurado por defecto en *mobile*. Tal y como se comprueba a nivel de red, se trata de la interfaz de *loopback* del propio equipo *host* en el que corre el software de análisis.

#### 4.5.4.1 Análisis de canales lógicos de control

Los canales lógicos de control o CCCH se ubican en el *slot* temporal 0 de la frecuencia patrón de cada antena y transportan información relevante que deben conocer todos los terminales móviles que campean en la red. Los canales FCCH y SCH no se muestran como tramas sino que la información que envían se muestra en el GSMTAP Header como se observa en la Ilustración 35.

Por lo tanto, mientras no se produzca ninguna comunicación ni procedimiento dentro de la estación base, se sucederán tramas BCCH y PAGCH. Para una transmisión

completa de cada uno de éstos canales son necesarios 4 *slots* temporales por lo que el WireShark los agrupará para formar una unidad de GSMTAP. Por lo tanto tendremos secuencias de una trama BCCH y nueve PAGCH tal y como se observaba en el apartado 2.2.1.2. En la Ilustración 36 observamos una trama PAGCH de ejemplo.

```
GSM TAP Header, ARFCN: 989 (Downlink), TS: 0, Channel: PCH (0)
Version: 2
Header length: 16 bytes
Payload Type: GSM Um (MS<->BTS) (1)
Time Slot: 0
..00 0011 1101 1101 = ARFCN: 989  FFCH
.0.. .... .... .... = Uplink: 0
Signal/Noise Ratio (dB): 190
Signal Level (dBm): 0
GSM Frame Number: 846204  SCH
Channel Type: PCH (5)
Antenna Number: 0
Sub-Slot: 0
```

Ilustración 35: Cabecera GSMTAP

Aunque existen algunas variaciones, la gran mayoría de las tramas de asignación tienen los mismos campos que en la captura. Recordemos que esta trama se produce en sentido descendente y sirve para localizar los móviles cuando tienen una llamada entrante, para comunicarle una repuesta a alguna petición de servicio o para solicitar algún procedimiento al terminal. El terminal móvil únicamente captura las tramas que provienen de la estación base por lo que no se pueden observar las respuestas emitidas por los demás terminales que se encuentran en la red.

```

  Channel Needed
    ..00 .... = Channel 1: Any channel (0)
    00.. .... = Channel 2: Any channel (0)
  Mobile Identity - Mobile Identity 1 - TMSI/P-TMSI (0xf240e45f)
    Length: 5
    1111 .... = Unused
    .... 0... = Odd/even indication: Even number of identity digits
    .... .100 = Mobile Identity Type: TMSI/P-TMSI (4)
    TMSI/P-TMSI: 0xf240e45f
  P1 Rest Octets
    L... ..: NLN(PCH): Not present
    .L.. ..: Priority 1: Not present
    ..L. ..: Priority 2: Not present
    ...L ..: Group Call Information: Not present
    .... L...: Packet Page Indication 1: For RR connection establishment
    .... .L...: Packet Page Indication 2: For RR connection establishment
    Padding Bits: default padding
```

Ilustración 36: Trama PAGCH

Para que el móvil afectado sea consciente de que se dirige hacia él, en el campo *Mobile Identity* se indica bien su TMSI o su IMSI. Vemos también el que en el campo *Channel Needed* no se solicita ningún canal. Un poco más abajo se puede leer *For RR connection establishment* que indica que la trama es un simple reconocimiento para que el terminal indique si sigue en la misma celda y se encuentra operativo.

Las tramas del canal de control BCCH ofrecen información acerca de los parámetros de la estación base. Hay varios tipos de trama que se van sucediendo y que transmiten diversa información. Los terminales siempre se mantienen a la escucha del canal para conocer las propiedades de la red como pueden ser el número de retransmisiones

máximo, los números de identificación de celda, niveles de señal y ruido o información sobre las antenas adyacentes.

```

  ▾ Neighbour Cell Description 2 - Extended BCCH Frequency List
    .10. .... = Multiband Reporting: 2
    ...1 .... = BA-IND: 1
    1... 111. = Format Identifier: variable bit map (0x47)
    List of ARFCNs = 525 527 539 542 544 555
  
```

#### Ilustración 37: Campo 'Celdas vecinas' en trama BCCH

En las capturas Ilustración 37 e Ilustración 38, se puede comprobar cómo el terminal recibe información sobre la celda a la que está asociado así como de otras celdas adyacentes. Todos estos parámetros resultan necesarios para la configuración de transmisión y recepción de la señales radio así como de variaciones en los protocolos de intercambio de información entre estación base y terminal.

La última trama que podemos capturar con nuestro analizador dentro de los CCCH es la de asignación inmediata. Es un procedimiento especial para asignar un canal de tráfico dedicado a un terminal que necesita realizar una llamada, que tiene una llamada entrante o que quiere realizar algún procedimiento de asociación o actualización de posición. Aunque se encuentra dentro de los canales PAGCH, se conoce con el nombre de Asociación Inmediata.

```

  ▾ Cell Identity - CI (2401)
    Cell CI: 0x0961 (2401)
  ▾ Location Area Identification (LAI)
    ▾ Location Area Identification (LAI) - 214/07/3906
      Mobile Country Code (MCC): Spain (214)
      Mobile Network Code (MNC): Telefonica Moviles Espana, SAU (07)
      Location Area Code (LAC): 0x0f42 (3906)
  ▾ Control Channel Description
    1... .... = MSCR: MSC is Release '99 onwards (1)
    .1.. .... = ATT: MSs in the cell shall apply IMSI attach and detach procedure (1)
    ..00 1... = BS_AG_BLK_RES: 1
    .... .000 = CCCH-CONF: 1 basic physical channel used for CCCH, not combined with SDCCCHs (0)
    .00. .... = CBQ3: Iu mode not supported (0)
    .... .011 = BS-PA-MFRMS: 3
    T3212: 40
  ▾ Cell Options (BCCH)
    .1.. .... = PWRC: True
    ..01 .... = DTX (BCCH): The MSs shall use uplink discontinuous transmission (1)
    .... 0111 = Radio Link Timeout: 32 (7)
  ▾ Cell Selection Parameters
    011. .... = Cell Reselection Hysteresis: 3
    ...0 0101 = MS TXPWR MAX CCH: 5
    0... .... = ACS: False
    .0.. .... = NECI: 0
    ..00 1000 = RXLEV-ACCESS-MIN: -103 <= x < -102 dBm (8)
  ▾ RACH Control Parameters
    10.. .... = Max retrans: Maximum 4 retransmissions (2)
    ..10 11.. = Tx-integer: 16 slots used to spread transmission (11)
    .... ..0. = CELL_BARR_ACCESS: The cell is not barred (0)
    .... ...1 = RE: True
    0000 0000 0000 0000 = ACC: 0x0000
  
```

#### Ilustración 38: Trama BCCH con parámetros e identificación de celda

Puede observarse además en la Ilustración 39 que la estación base envía al terminal todos los datos necesarios para acceder al canal dedicado: tipo de canal, *slot* temporal, secuencia de entrenamiento a utilizar, datos para realizar el salto en frecuencia... Además le indica la codificación a nivel físico en el campo *Request Reference*. Por último, para que el terminal se sincronice de forma correcta con la estación base, se le indica su posición y el retardo a utilizar debido a tiempo de propagación de las señales inalámbricas.

```

▽ Dedicated mode or TBF
  0000 .... = Dedicated mode or TBF: This message assigns a dedicated mode resource (0)
▽ Channel Description
  0111 1... = SDCCH/8 + SACCH/C8 or CBCH (SDCCH/8), Subchannel 7
  .... .001 = Timeslot: 1
  111. .... = Training Sequence: 7
  ...1 .... = Hopping channel: Yes
  Hopping channel: MAIO 0
  Hopping channel: HSN 54
▽ Request Reference
  Random Access Information (RA): 10
  0110 1... = T1': 13
  .... .001 011. .... = T3: 11
  ...0 1101 = T2: 13
  [RFN: 18473]
▽ Timing Advance
  Timing advance value: 0
▽ Mobile Allocation
  Length: 1
  Bitmap of increasing ARFCNs included in the Mobile Allocation: 11100000

```

**Ilustración 39: Captura de asignación inmediata**

#### 4.5.4.2 Estudio de procedimientos realizados por el terminal dentro de la red

Gracias al analizador, es posible conocer los detalles de los diferentes procesos de comunicación que se realizan entre la estación base y los móviles asociados a la misma. A continuación se verán las sucesiones de tramas y la información más relevante de las mismas cuando el terminal se asocia a la red, envía un SMS o recibe una llamada. Este análisis facilita la comprensión de las tramas estudiadas en la descripción del estándar GSM.

##### 4.5.4.2.1 Primer acceso a la red

Cuando un terminal necesita acceder a la red, lo primero que necesita es acceder a un canal dedicado. Tras escuchar las tramas *broadcast* necesarias de la estación base envía una petición y la estación base le contestará con una Asignación Inmediata proporcionando información sobre el canal dedicado y las características de la comunicación. Tras esto y según indica el diagrama de la Ilustración 40, se producirá la comunicación por el canal dedicado con la sucesión de tramas mostrada en la Ilustración 41.

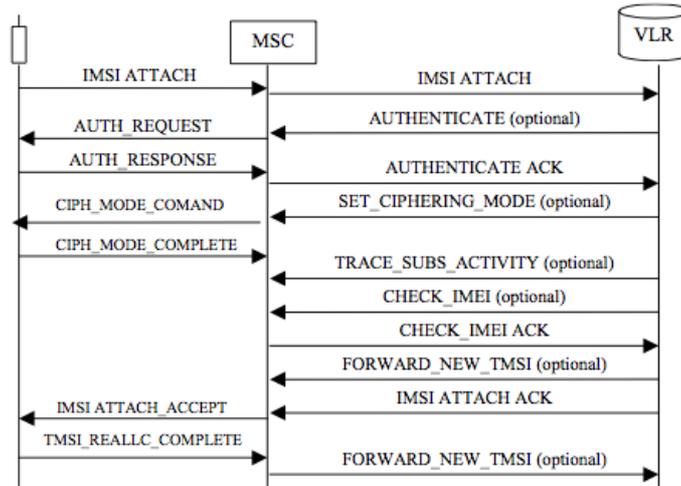


Ilustración 40: Diagrama de flujo para acceso a la red

41	1.550900	127.0.0.1	127.0.0.1	LAPDm	81 U, func=UI (DTAP) (RR) Measurement Report
42	1.550912	127.0.0.1	127.0.0.1	LAPDm	81 U P, func=SABM(DTAP) (MM) Location Updating Request
45	1.768974	127.0.0.1	127.0.0.1	LAPDm	81 U, func=UI
46	1.844061	127.0.0.1	127.0.0.1	LAPDm	81 U, func=UI (DTAP) (RR) System Information Type 5
47	2.004017	127.0.0.1	127.0.0.1	LAPDm	81 U F, func=UA(DTAP) (MM) Location Updating Request
48	2.239929	127.0.0.1	127.0.0.1	LAPDm	81 I, N(R)=0, N(S)=0(DTAP) (RR) Ciphering Mode Command
49	2.239946	127.0.0.1	127.0.0.1	LAPDm	81 S, func=RR, N(R)=1
50	2.239958	127.0.0.1	127.0.0.1	LAPDm	81 I, N(R)=1, N(S)=0(DTAP) (RR) Ciphering Mode Complete
51	2.475010	127.0.0.1	127.0.0.1	LAPDm	81 U, func=UI
52	2.551632	127.0.0.1	127.0.0.1	LAPDm	81 U, func=UI (DTAP) (RR) Measurement Report
53	2.710061	127.0.0.1	127.0.0.1	LAPDm	81 I, N(R)=1, N(S)=1(DTAP) (MM) Location Updating Accept
54	2.710079	127.0.0.1	127.0.0.1	LAPDm	81 S, func=RR, N(R)=2
55	2.946296	127.0.0.1	127.0.0.1	LAPDm	81 I, N(R)=1, N(S)=2(DTAP) (RR) Channel Release
56	2.946313	127.0.0.1	127.0.0.1	LAPDm	81 S, func=RR, N(R)=3
57	2.946325	127.0.0.1	127.0.0.1	LAPDm	81 U P, func=DISC
58	3.180978	127.0.0.1	127.0.0.1	LAPDm	81 U, func=UI
59	3.416084	127.0.0.1	127.0.0.1	LAPDm	81 U F, func=UA

Ilustración 41: Procedimiento de acceso a la red

Las dos primeras tramas enviadas por el terminal hacia la estación base contienen por una parte medidas (trama 41, Ilustración 42) realizadas en el interfaz radio y por otra (trama 42, Ilustración 43) una solicitud de actualización de posición para que la estación conozca las características del terminal.

```

Measurement Results
0... .... = BA-USED: 0
.0.. .... = DTX-USED: DTX was not used
..00 0000 = RXLEV-FULL-SERVING-CELL: < -110 dBm (0)
0... .... = 3G-BA-USED: 0
.1.. .... = MEAS-VALID: The measurement results are not valid
RXLEV-SUB-SERVING-CELL: Unknown (64)
.000 .... = RXQUAL-FULL-SERVING-CELL: BER < 0.2%, Mean value 0.14% (0)
.... 000. = RXQUAL-SUB-SERVING-CELL: BER < 0.2%, Mean value 0.14% (0)
.... ...1 11.. .... = NO-NCCELL-M: Neighbour cell information not available for serving cell (7)
    
```

Ilustración 42: Trama 41 con medidas en el interfaz radio

```

  ▾ Location Updating Type - IMSI attach
    .... 0... = Follow-On Request (FOR): No follow-on request pending
    .... .0.. = Spare bit(s): 0
    .... ..10 = Updating Type: IMSI attach
  ▾ Location Area Identification (LAI)
    ▾ Location Area Identification (LAI) - 214/07/3906
      Mobile Country Code (MCC): Spain (214)
      Mobile Network Code (MNC): Telefonica Moviles Espana, SAU (07)
      Location Area Code (LAC): 0x0f42 (3906)
  ▾ Mobile Station Classmark 1
    ▾ Mobile Station Classmark 1
      0... .... = Spare: 0
      .01. .... = Revision Level: Used by GSM phase 2 mobile stations (1)
      ...0 .... = ES IND: Controlled Early Classmark Sending option is not implemented in the MS
      .... 0... = A5/1 algorithm supported: encryption algorithm A5/1 available
      .... .011 = RF Power Capability: class 4 (3)
  ▾ Mobile Identity - TMSI/P-TMSI (0x6c0d7625)
    Length: 5
    1111 .... = Unused
    .... 0... = Odd/even indication: Even number of identity digits
    .... .100 = Mobile Identity Type: TMSI/P-TMSI (4)
    TMSI/P-TMSI: 0x6c0d7625

```

**Ilustración 43: Trama 42 con datos sobre la interfaz móvil**

Posteriormente, mediante la trama 45, la estación base envía un acuse de recibo de las tramas anteriores. La trama 46 se encapsula el envío de información adicional sobre las celdas candidatas para que el móvil conozca las antenas que tiene alrededor y la 47 confirma que procede a cursar la solicitud de actualización de posición. Tras esto, mediante la trama 48 se envía la solicitud de cifrado de las comunicaciones, el móvil confirma que la recibe mediante la 49 e indica que se ha completado el procedimiento con la 50.

```

  ▶ Protocol Discriminator: Mobility Management messages
    00.. .... = Sequence number: 0
    ..00 0010 = DTAP Mobility Management Message Type: Location Updating Accept (0x02)
  ▾ Location Area Identification (LAI)
    ▾ Location Area Identification (LAI) - 214/07/3906
      Mobile Country Code (MCC): Spain (214)
      Mobile Network Code (MNC): Telefonica Moviles Espana, SAU (07)
      Location Area Code (LAC): 0x0f42 (3906)

```

**Ilustración 44: Trama 53 de confirmación del proceso de actualización de posición**

El siguiente paso es la confirmación de recibo por parte de la estación base en la trama 51 y la confirmación del proceso de actualización de posición en la 53 (Ilustración 44). La trama 52 se trata de una medida periódica que realizar el móvil de los parámetros radio. Por último el terminal confirma el recibo en la trama 54 y se procede a cerrar el canal de comunicación, y sus correspondientes reconocimientos, con la sucesión de las tramas 55, 56, 57, 58 y 59.

#### 4.5.4.2.2 Realización de llamadas de voz

Vamos a ver dos ejemplos, primero una llamada saliente desde el analizador y luego otra entrante al mismo. Se comentará el procedimiento y las diferencias entre ambos.

##### Llamada saliente:

El programa *mobile*, que permite controlar el móvil de forma remota desde una consola de comandos, cuenta con un procedimiento para iniciar llamadas de voz. Para ello debe introducirse el comando

```
OsmocomBB# call +YYXXXXXXXXXX
```

donde YY es el código del país y las X's los dígitos del número al que desea llamarse. Antes de realiza el paso, iniciamos la captura dentro de WireShark para poder analizar los datos con detalle.

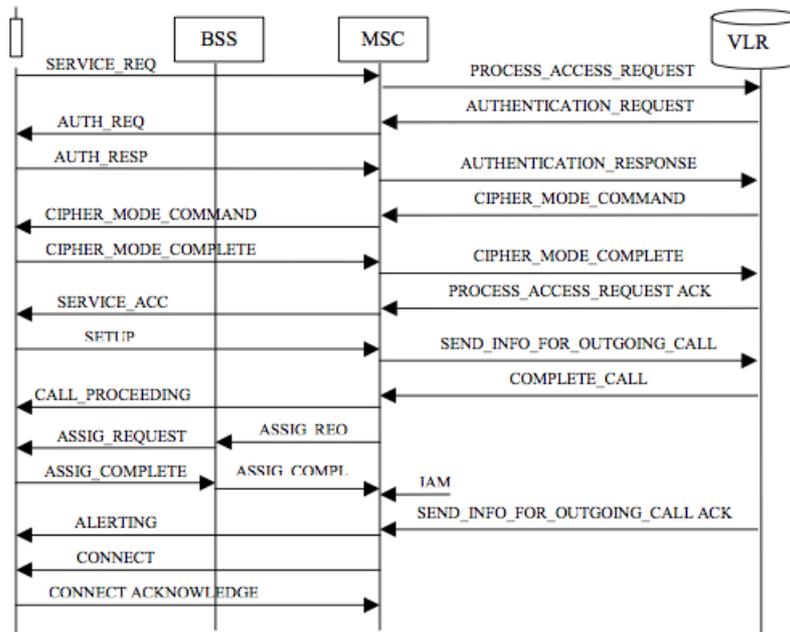


Ilustración 45: Diagrama de flujo de llamada entrante

En la Ilustración 45 se puede observar el intercambio de primitivas que se lleva a cabo en el tramo de la red que se está analizando. Bien es cierto que en nuestras capturas faltan las tramas de autenticación debido a que los casos en los que debe llevarse a cabo el proceso dependen del operador. De esta forma puede haber ocurrido que no para el proveedor utilizado no sea obligatoria la autenticación antes de cada llamada o bien que otro procedimiento haya realizado una autenticación de forma reciente y no sea necesario realizar otra hasta pasado un intervalo temporal fijado por el operador.

Una vez finalizada la captura, vamos a analizar las tramas obtenidas y a describir los procedimientos más importantes y la información contenida en las mismas para entender el funcionamiento del estándar. En primer lugar tenemos como en todos los procedimientos la Asignación Inmediata del canal dedicado. Se intercambian medidas y se realiza la petición del servicio. La sucesión se puede observar en la Ilustración 46.

218	7.951884	127.0.0.1	127.0.0.1	LAPDm	81 U, func=UI (DTAP) (RR) Measurement Report
219	7.951897	127.0.0.1	127.0.0.1	LAPDm	81 U P, func=SABM (DTAP) (MM) CM Service Request
222	8.049712	127.0.0.1	127.0.0.1	LAPDm	81 U, func=UI
223	8.198976	127.0.0.1	127.0.0.1	LAPDm	81 U, func=UI (DTAP) (RR) System Information Type 5
224	8.284906	127.0.0.1	127.0.0.1	LAPDm	81 U F, func=UA (DTAP) (MM) CM Service Request
225	8.521024	127.0.0.1	127.0.0.1	LAPDm	81 I, N(R)=0, N(S)=0 (DTAP) (RR) Ciphering Mode Command
226	8.521044	127.0.0.1	127.0.0.1	LAPDm	81 S, func=RR, N(R)=1
227	8.521057	127.0.0.1	127.0.0.1	LAPDm	81 I, N(R)=1, N(S)=0 (DTAP) (RR) Ciphering Mode Complete
228	8.667728	127.0.0.1	127.0.0.1	LAPDm	81 U, func=UI (DTAP) (RR) System Information Type 6
229	8.755837	127.0.0.1	127.0.0.1	LAPDm	81 U, func=UI
230	8.952988	127.0.0.1	127.0.0.1	LAPDm	81 U, func=UI (DTAP) (RR) Measurement Report
231	8.991245	127.0.0.1	127.0.0.1	LAPDm	81 S, func=RR, N(R)=1
232	8.991263	127.0.0.1	127.0.0.1	LAPDm	81 I, N(R)=1, N(S)=1 (DTAP) (CC) Setup
233	9.139863	127.0.0.1	127.0.0.1	LAPDm	81 U, func=UI (DTAP) (RR) System Information Type 5
234	9.227017	127.0.0.1	127.0.0.1	LAPDm/GSM	81 I, N(R)=2, N(S)=1 (DTAP) (CC) Call Proceeding (GSM MAP) invoke
235	9.227064	127.0.0.1	127.0.0.1	LAPDm	81 S, func=RR, N(R)=2
236	9.461705	127.0.0.1	127.0.0.1	LAPDm	81 U, func=UI
237	9.609838	127.0.0.1	127.0.0.1	LAPDm	81 U, func=UI (DTAP) (RR) System Information Type 6
238	9.697886	127.0.0.1	127.0.0.1	LAPDm	81 I, N(R)=2, N(S)=2 (Fragment)
239	9.697904	127.0.0.1	127.0.0.1	LAPDm	81 S, func=RR, N(R)=3
240	9.932962	127.0.0.1	127.0.0.1	LAPDm	81 I, N(R)=2, N(S)=3 (DTAP) (RR) Assignment Command
241	9.932986	127.0.0.1	127.0.0.1	LAPDm	81 S, func=RR, N(R)=4
242	9.933001	127.0.0.1	127.0.0.1	LAPDm	81 U, func=UI (DTAP) (RR) Measurement Report
243	9.933038	127.0.0.1	127.0.0.1	LAPDm	81 U P, func=SABM
244	10.046545	127.0.0.1	127.0.0.1	LAPDm	81 U, func=UI

Ilustración 46: Tramas iniciales para el establecimiento de llamada saliente

Una vez finalizada la captura, vamos a analizar las tramas obtenidas y a describir los procedimientos más importantes y la información contenida en las mismas para entender el funcionamiento del estándar. En primer lugar tenemos como en todos los procedimientos la Asignación Inmediata del canal dedicado, cuya respuesta se puede ver en la trama 224. Se intercambian medidas y se realiza la petición del servicio.

```

  ▶ Protocol Discriminator: Mobility Management messages
    00.. .... = Sequence number: 0
    ..10 0100 = DTAP Mobility Management Message Type: CM Service Request (0x24)
  ▶ Ciphering Key Sequence Number
  ▼ CM Service Type
    .... 0001 = Service Type: (1) Mobile originating call establishment or packet mode connection establishment
  ▶ Mobile Station Classmark 2
  ▼ Mobile Identity - TMSI/P-TMSI (0x6c0d7625)
    Length: 5
    1111 .... = Unused
    .... 0... = Odd/even indication: Even number of identity digits
    .... .100 = Mobile Identity Type: TMSI/P-TMSI (4)
    TMSI/P-TMSI: 0x6c0d7625

```

#### Ilustración 47: Trama de solicitud de servicio de llamada saliente

La trama contiene información acerca del terminal, sus características (*Mobile Station Classmark*) y el tipo de servicio. La estación base confirma el recibo con la trama 222 y procede a gestionar la petición con la 224. Las tramas 225 y 227, al igual que para el caso anterior, son parte de la negociación de claves a usar en la comunicación. De aquí en adelante se obviará el intercambio de medidas y las confirmaciones de recibo que se establecen para el mantenimiento de la comunicación al ser redundante y no aportar información sobre el funcionamiento.

La siguiente trama importante es la 232, que es enviada por el terminal con información acerca de las características que tendrá la llamada. Como se observa en la Ilustración 48, se envían el número de destino y los protocolos de control de llamada a utilizar.

```

  ▶ Protocol Discriminator: Call Control; call related SS messages
    01.. .... = Sequence number: 1
    ..00 0101 = DTAP Call Control Message Type: Setup (0x05)
  ▶ Bearer Capability 1 - (MS supports at least full rate speech version 1 and half rate speech version 1. MS has a greater preference for full rate speech)
  ▶ Called Party BCD Number - (34675115348)
  ▶ Call Control Capabilities

```

#### Ilustración 48: Trama de configuración de llamada saliente

Mediante la trama 234 la estación base indica al terminal que está invocando el proceso de llamada y la 240, enviada también en sentido descendente, indica que se está gestionando el acceso al canal y se están configurando los elementos necesarios para que sea establecido. El móvil analiza los parámetros del canal, la potencia a emitir, las frecuencias... y envía en la trama 254 una confirmación de que la asignación es completa y que ya puede establecerse la llamada. Una vez hecho esto la estación base y los elementos del *backbone* de la red GSM comienzan a encaminar la llamada y establecer las rutas para que pueda llevarse a cabo. Tal y como puede verse en las tramas de la Ilustración 49, cuando el móvil destino está localizado y los elementos intermedios configurados la estación base avisa al terminal utilizando la trama 288 de *Alerting* de que el destinatario ya está recibiendo la llamada y sólo tiene que descolgar para aceptarla. En las tramas 297 y 299 se indica al terminal que el llamado ha descolgado y el terminal acepta la información.

287	19.939463	127.0.0.1	127.0.0.1	LAPDm	81 U, func=UI (DTAP) (RR) Measurement Report
288	20.246657	127.0.0.1	127.0.0.1	LAPDm	81 I, N(R)=1, N(S)=0 (DTAP) (CC) Alerting
289	20.246708	127.0.0.1	127.0.0.1	LAPDm	81 S, func=RR, N(R)=1
297	22.388799	127.0.0.1	127.0.0.1	LAPDm	81 I, N(R)=1, N(S)=1 (DTAP) (CC) Connect
298	22.388846	127.0.0.1	127.0.0.1	LAPDm	81 S, func=RR, N(R)=2
299	22.388859	127.0.0.1	127.0.0.1	LAPDm	81 I, N(R)=2, N(S)=1 (DTAP) (CC) Connect Acknowledge

#### Ilustración 49: Tramas de establecimiento de llamada saliente

Debido a que las tramas de tráfico de voz durante la conversión están cifradas y el disector de GSMTAP no las reconoce, sólo se muestra el intercambio de tramas de control de conexión y reporte de medidas del canal. Por tanto, se muestra en la Ilustración 50 el proceso de desconexión de los terminales.

310	25.605897	127.0.0.1	127.0.0.1	LAPDm	81 I, N(R)=2, N(S)=2(OTAP) (CC) Disconnect
311	25.605943	127.0.0.1	127.0.0.1	LAPDm	81 S, func=RR, N(R)=3
312	25.605955	127.0.0.1	127.0.0.1	LAPDm	81 I, N(R)=3, N(S)=2(OTAP) (CC) Release
313	25.671603	127.0.0.1	127.0.0.1	LAPDm	81 U, func=UI(OTAP) (RR) System Information Type 5
314	25.766719	127.0.0.1	127.0.0.1	LAPDm	81 S, func=RR, N(R)=3
315	25.826907	127.0.0.1	127.0.0.1	LAPDm	81 I, N(R)=3, N(S)=3(OTAP) (CC) Release Complete

Ilustración 50: Tramas de desconexión de la llamada saliente

Debido a que es el llamado, es decir, el que cuelga la llamada, la estación base envía un *Disconnect* en la trama 310. En ella, se indica la razón de la desconexión, que en este caso es *Normal call clearing* lo que indica que uno de los terminales ha pulsado el botón de colgar la llamada. Entonces el terminal comienza un proceso de liberación de la llamada (trama 312) que la base acepta (trama 315). Por último, la estación envía una trama indicando que el canal está liberado para el terminal pueda dar por terminada la comunicación y vuelva a operar manteniéndose a la espera.

Llamada entrante:

Al igual que *mobile* permitía controlar de forma remota el terminal para realizar una llamada, la consola también alertará de una llamada entrante. En esta ocasión, para dar al usuario a conocer que el analizador está recibiendo una llamada, se muestra lo siguiente en la consola, donde XXXXXXXXXX será la identidad del número llamante:

% Incoming call (from 0-XXXXXXXXXX)

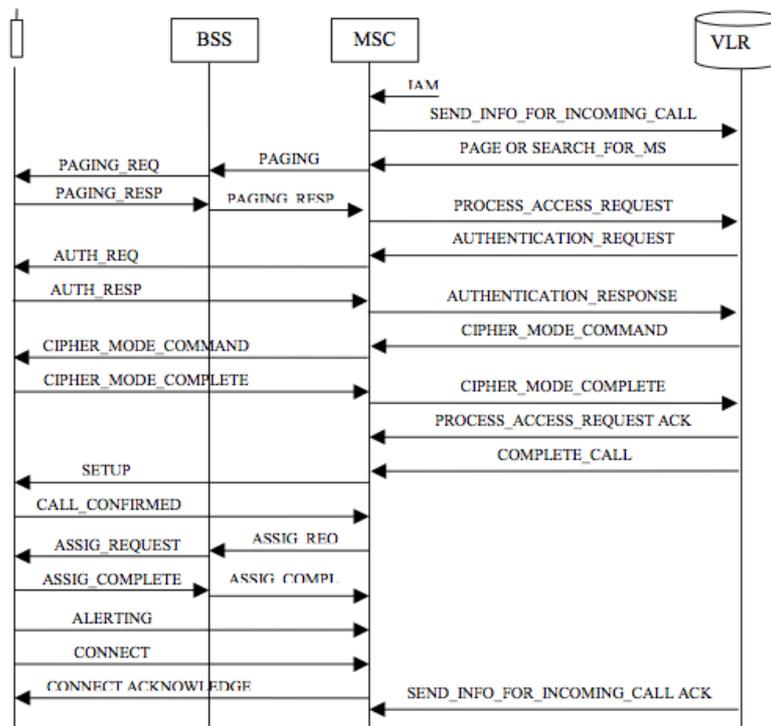


Ilustración 51: Diagrama de flujo llamada entrante

En este momento se ha de escribir el comando *call answer* para descolgar la llamada. Tras colgar la llamada se parará la captura para comprobar los resultados y analizar el intercambio de tramas. Se observa en la Ilustración 51 el diagrama de flujo que

conlleva una operación de llamada entrante. A continuación se mostrarán las tramas que hemos capturado y comprobando que coinciden con las que, salvo el procedimiento de autenticación como en el caso anterior, describe el estándar GSM.

421	11.299574	127.0.0.1	127.0.0.1	LAPDm	81 U, func=UI (DTAP) (RR) Measurement Report
422	11.299586	127.0.0.1	127.0.0.1	LAPDm	81 U P, func=SABM(DTAP) (RR) Paging Response
423	11.324683	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR) Paging Request Type 1
424	11.360637	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR) Paging Request Type 1
425	11.571197	127.0.0.1	127.0.0.1	LAPDm	81 U F, func=UA (DTAP) (RR) Paging Response
426	11.646204	127.0.0.1	127.0.0.1	LAPDm	81 U, func=UI (DTAP) (RR) System Information Type 5
427	11.807196	127.0.0.1	127.0.0.1	LAPDm	81 I, N(R)=0, N(S)=0 (DTAP) (RR) Ciphering Mode Command
428	11.807213	127.0.0.1	127.0.0.1	LAPDm	81 S, func=RR, N(R)=1
429	11.807226	127.0.0.1	127.0.0.1	LAPDm	81 I, N(R)=1, N(S)=0 (DTAP) (RR) Ciphering Mode Complete

Ilustración 52: Tramas iniciales de establecimiento de llamada entrante

Obviando nuevamente las comprobaciones periódicas de conexión y los reconocimientos a nivel de enlace que se aprecian en la Ilustración 52, tenemos la primera trama diferente al caso anterior. *Paging Response* es la respuesta del terminal a la asignación de canal que en este caso no ha sido solicitada por él sino que la base ha localizado el terminal para indicarle que tiene información para él. El contenido de la trama es muy similar a la petición de servicio y se indica la identidad del móvil y sus características. La estación responde aceptando los parámetros con el mismo tipo de trama y se pasa a la negociación de claves necesaria para establecer el canal de voz.

432	12.277336	127.0.0.1	127.0.0.1	LAPDm	81 I, N(R)=1, N(S)=1 (DTAP) (CC) Setup
433	12.277383	127.0.0.1	127.0.0.1	LAPDm	81 S, func=RR, N(R)=2
434	12.277395	127.0.0.1	127.0.0.1	LAPDm	81 I, N(R)=2, N(S)=1 (DTAP) (CC) Call Confirmed
438	12.748359	127.0.0.1	127.0.0.1	LAPDm	81 S, func=RR, N(R)=2
439	12.748376	127.0.0.1	127.0.0.1	LAPDm	81 I, N(R)=2, N(S)=2 (DTAP) (CC) Alerting
440	12.984262	127.0.0.1	127.0.0.1	LAPDm	81 S, func=RR, N(R)=3
444	13.303809	127.0.0.1	127.0.0.1	LAPDm	81 U, func=UI (DTAP) (RR) Measurement Report
445	13.455620	127.0.0.1	127.0.0.1	LAPDm	81 I, N(R)=3, N(S)=3 (DTAP) (RR) Assignment Command
446	13.455637	127.0.0.1	127.0.0.1	LAPDm	81 S, func=RR, N(R)=4
459	13.760165	127.0.0.1	127.0.0.1	LAPDm	81 U F, func=UA
460	13.760181	127.0.0.1	127.0.0.1	LAPDm	81 I, N(R)=0, N(S)=0 (DTAP) (RR) Assignment Complete
461	13.783671	127.0.0.1	127.0.0.1	LAPDm	81 U, func=UI

Ilustración 53: Tramas de establecimiento de llamada entrante

Según puede comprobarse en la Ilustración 53, la trama 432 es, como para el caso de una llamada saliente, la trama de *Setup*, pero enviada desde la estación al móvil y con la identidad del llamante en este caso. En lugar de una aceptación de la configuración por parte de la estación base, el terminal acepta la llamada (trama 434), aunque aun no se haya descolgado, e indica los parámetros de configuración que utilizará. Posteriormente cuando ya está totalmente preparado para establecer la comunicación, envía la trama de *Alerting* (trama 439) al usuario de que tiene una llamada.

Con el *Assignment Command* (trama 445) y *Assignment Complete* (trama 460) se establece la comunicación entre las partes al conocer ambos extremos los parámetros de configuración a utilizar. Posteriormente, el usuario llamado descuelga el teléfono (Ilustración 54).

471	16.135665	127.0.0.1	127.0.0.1	LAPDm	81 I, N(R)=0, N(S)=1 (DTAP) (CC) Connect
472	16.262185	127.0.0.1	127.0.0.1	LAPDm	81 S, func=RR, N(R)=2
473	16.305328	127.0.0.1	127.0.0.1	LAPDm	81 U, func=UI (DTAP) (RR) System Information Type 5
474	16.359164	127.0.0.1	127.0.0.1	LAPDm	81 I, N(R)=2, N(S)=0 (DTAP) (CC) Connect Acknowledge

Ilustración 54: Tramas de conexión de llamada entrante

Cuando se produce el descuelgo de la llamada, el terminal móvil transmite una trama de conexión de llamada y posteriormente la estación base confirma dicha conexión. Al igual que para el caso anterior, no es posible visualizar las tramas de tráfico de voz ya que el analizador no cuenta con el software necesario.

471	16.135665	127.0.0.1	127.0.0.1	LAPDm	81 I, N(R)=0, N(S)=1 (DTAP) (CC) Connect
472	16.262185	127.0.0.1	127.0.0.1	LAPDm	81 S, func=RR, N(R)=2
473	16.305328	127.0.0.1	127.0.0.1	LAPDm	81 U, func=UI (DTAP) (RR) System Information Type 5
474	16.359164	127.0.0.1	127.0.0.1	LAPDm	81 I, N(R)=2, N(S)=0 (DTAP) (CC) Connect Acknowledge

Ilustración 55: Tramas de desconexión de llamada entrante

Al ser el terminal remoto quien cuelga la llamada, el orden de las tramas para la desconexión es el mismo que para el caso anterior.

#### 4.5.4.2.3 Envío y recepción de SMS

Para realizar la prueba de envío de mensajes mediante el servicio SMS implementado en el estándar GSM se ha realizado el envío de un SMS entrante al analizador y éste a su vez ha realizado un envío de SMS a otro terminal. El procedimiento de envío de mensajería corta viene definido por la norma GSM 03.40 [20] de estándar. El texto de ambos SMS es "Hola". A continuación analizaremos los diferentes casos y comprobaremos la sucesión de tramas del protocolo y sus diferencias.

##### SMS saliente:

Para enviar un SMS es necesario introducir en la consola de control del analizador el comando

```
OsmocomBB# sms +YYXXXXXXXXXX Texto
```

YY corresponde al código del país, las X's al número destinatario del mensaje y a continuación el texto que se desea enviar. Aunque el intercambio de tramas es algo más sencillo que para el caso de las llamadas de voz, muchas de las tramas son similares o incluso algunas de ellas iguales. Una de las diferencias es el tipo de servicio solicitado (Ilustración 56).

```

▼ CM Service Type
  .... 0100 = Service Type: (4) Short message service

```

**Ilustración 56: Petición de servicio SMS**

Empieza de nuevo con la asignación del canal por parte de la estación base y la petición de servicio del terminal. Aunque como se puede observar en la Ilustración 57, en éste caso el código de la petición corresponde al servicio de mensajería corta. Al igual que en casos anteriores, la estación base acepta la petición y repite los parámetros indicados por el terminal para confirmarlos. La siguiente acción es idéntica a los procedimientos ya estudiados y consiste en el intercambio de claves.

398	10.671395	127.0.0.1	127.0.0.1	GSM SMS	81 I, N(R)=0, N(S)=1(DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to Network)
399	10.907261	127.0.0.1	127.0.0.1	LAPDm	81 I, N(R)=2, N(S)=0(DTAP) (SMS) CP-ACK
404	11.378414	127.0.0.1	127.0.0.1	LAPDm	81 I, N(R)=2, N(S)=1(DTAP) (SMS) CP-DATA (RP) RP-ACK (Network to MS)
405	11.378461	127.0.0.1	127.0.0.1	LAPDm	81 S, func=RR, N(R)=2
406	11.378474	127.0.0.1	127.0.0.1	LAPDm	81 I, N(R)=2, N(S)=2(DTAP) (SMS) CP-ACK

**Ilustración 57: Tramas de datos SMS saliente**

Las tramas anteriores conforman la parte propia de transmisión de información en el protocolo SMS. En primer lugar, el terminal que origina el mensaje envía la siguiente información mediante la trama 308.

En la trama de la Ilustración 58 se puede observar que existen dos destinatarios diferentes. El estándar define que el SMS ha de ser dirigido hacia el centro de mensajes de la red del operador, que centraliza y redirige el mensaje hacia el terminal destino. De ésta forma, el gestor de la red puede almacenar el mensaje si no puede ser enviado y posee un mayor control para garantizar que la información sea entregada. Siguiendo la normal GSM 03.40, el número del destinatario y el texto se encuentran en la parte final de la trama. Además se añaden parámetros de configuración como acuse de recibo, posponer la entrega en caso de no poder realizarse... La siguiente trama es la confirmación por parte de la estación base de que ha recibido la información completa y sin errores.

```

▼ GSM A-I/F RP - RP-DATA (MS to Network)
  Message Type RP-DATA (MS to Network)
  ▶ RP-Message Reference
  ▶ RP-Origination Address
  ▶ RP-Destination Address - (34609090909)
  ▶ RP-User Data
▼ GSM SMS TPDU (GSM 03.40) SMS-SUBMIT
  0... .... = TP-RP: TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER
  .0.. .... = TP-UDHI: The TP UD field contains only the short message
  ..0. .... = TP-SRR: A status report is not requested
  ...0 0... = TP-VPF: TP-VP field not present (0)
  .... .0.. = TP-RD: Instruct SC to accept duplicates
  .... ..01 = TP-MTI: SMS-SUBMIT (1)
  TP-MR: 0
  ▶ TP-Destination-Address - (34609090909)
  ▶ TP-PID: 0
  ▶ TP-DCS: 0
  TP-User-Data-Length: (4) depends on Data-Coding-Scheme
  ▼ TP-User-Data
    SMS text: Hola

```

Ilustración 58: Detalle de trama de datos SMS saliente

Por último la trama de información de servicio SMS *RP-ACK* (404) indica al terminal que la información ha sido entregada correctamente al destinatario de la misma. Con la 406, el móvil confirma que ha recibido la información anterior a nivel de conexión, es decir, con un reconocimiento simple.

408 11.613149	127.0.0.1	127.0.0.1	LAPDm	81 U, func=UI
409 11.849508	127.0.0.1	127.0.0.1	LAPDm	81 I, N(R)=1, N(S)=1(DTAP) (RR) Channel Release
410 11.849527	127.0.0.1	127.0.0.1	LAPDm	81 S, func=RR, N(R)=2

Ilustración 59: Tramas de desconexión del servicio SMS

Una vez realizado el proceso, la estación base procede a cerrar el canal de comunicación. En este caso, no es necesaria confirmación y el terminal da por finalizada la transacción.

### SMS entrante:

La confirmación de que se ha recibido un SMS se realiza mediante la presentación del siguiente mensaje en la consola de control del programa. Como hemos dicho anteriormente *mobile* realiza las funciones del interfaz de usuario en cualquier teléfono móvil.

```
% SMS from +YYXXXXXXXXXX Texto
```

Al analizar el procedimiento de recepción de un SMS se observan ciertas diferencias respecto al envío. Inicialmente, se recibe la asignación de canal dedicado tal y como ocurría en el apartado anterior con las llamadas entrantes. La estación asigna el canal, el terminal responde a la asignación y la base vuelve a enviar una trama confirmando los parámetros. Como viene siendo común a todos los procesos, se negocian las claves y ambos extremos están preparados para el intercambio de información de usuario (Ilustración 60).

210 6.356548	127.0.0.1	127.0.0.1	GSM SMS	81 I, N(R)=0, N(S)=1(DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to MS
211 6.356638	127.0.0.1	127.0.0.1	LAPDm	81 S, func=RR, N(R)=2
212 6.356651	127.0.0.1	127.0.0.1	LAPDm	81 I, N(R)=2, N(S)=0(DTAP) (SMS) CP-ACK

Ilustración 60: Tramas de información SMS entrante

En este momento la estación base envía el SMS al terminal de una forma similar al caso anterior con unas ligeras diferencias. Se observan los parámetros de envío y

también el texto al final de la trama. La diferencia en este caso es que aparece una dirección de origen, que corresponde al centro de mensajes del operador mediante el que se envía, y la dirección de origen del móvil que envió el mensaje. La trama siguiente es el reconocimiento de la información recibida por parte del terminal destinatario.

```

▼ GSM A-I/F RP - RP-DATA (Network to MS)
  Message Type RP-DATA (Network to MS)
  ▶ RP-Message Reference
  ▶ RP-Originating Address - (34656000311)
  ▶ RP-Destination Address
  ▶ RP-User Data
▼ GSM SMS TPDU (GSM 03.40) SMS-DELIVER
  0... .... = TP-RP: TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER
  .0.. .... = TP-UDHI: The TP UD field contains only the short message
  ..0. .... = TP-SRI: A status report shall not be returned to the SME
  .... .1.. = TP-MMS: No more messages are waiting for the MS in this SC
  .... ..00 = TP-MTI: SMS-DELIVER (0)
  ▶ TP-Originating-Address - (34      )
  ▶ TP-PID: 0
  ▶ TP-DCS: 0
  ▶ TP-Service-Centre-Time-Stamp
  TP-User-Data-Length: (4) depends on Data-Coding-Scheme
  ▼ TP-User-Data
    SMS text: Hola

```

**Ilustración 61: Detalle trama de datos SMS entrante**

Las tramas 217 y 218 son la confirmación por parte del terminal y el reconocimiento de la información por parte de la estación base respectivamente, del envío del mensaje. Esto servirá para que en el otro extremo se produzca la confirmación y el terminal que envió el SMS compruebe que efectivamente el mensaje ha llegado a su destino. El cierre de la conexión se realiza de forma unilateral por la estación base como ocurría en el caso de un SMS saliente.

## 4.6 Opciones y ventajas del proyecto OsmocomBB

Como se ha detallado en el capítulo, la plataforma OsmocomBB proporciona software de análisis de redes y protocolos GSM muy útiles para comprender el funcionamiento del estándar así como para realizar pruebas dentro una red. Aunque las redes convencionales pertenecientes a los operadores privados están fuertemente limitadas y es necesaria una tarjeta SIM propietaria para el acceso a las mismas, se han podido observar la mayoría de procedimientos del estándar salvo la captura del tráfico de voz debido a la encriptación de los datos. Por lo tanto sería una plataforma importante desde el punto de vista didáctico permitiendo observar de forma sencilla todos los entresijos de la tecnología GSM.

Además, al encontrarse el software dividido en varias partes (librerías) se reserva la opción de crear aplicaciones propietarias y/o específicas que permiten explotar todas las posibilidades y servicios disponibles en una red móvil GSM. Aunque en el presente proyecto no se ha profundizado en el desarrollo, se ha comprobado que gracias a los programas ya existentes podrían generarse interfaces más amigables con el fin de interpretar los datos obtenidos por las librerías de decodificación del estándar. Sería posible entonces trasladar los datos del terminal de texto plano a una interfaz gráfica así como la obtención de gráficas estadísticas sobre las tramas. También desde el proyecto OsmocomBB se está trabajando en librerías capaces de extraer los canales de audio. Estas conversaciones, aunque estén cifradas, podrían descifrarse ya que la

plataforma OsmocomBB cuenta también con los algoritmos de encriptación A5 utilizados en la implementación GSM, la cuál ha sido rota hace ya varios años [21].

Uno de los inconvenientes que hay que destacar es la imposibilidad de analizar tramas pertenecientes a protocolos GPRS debido a que los terminales compatibles que cuentan con el mencionado chip *Calypso* no soportan dicha tecnología y no son capaces de realizar procedimientos de dicho estándar. Recientemente los precursores del proyecto OsmocomBB están intentando modificar el software actual debido a que el modelo C123 de Motorola sí que podría conseguir interceptar y descifrar el tráfico GPRS [22]. Para ampliar las capacidades del analizador a la transmisión de datos, sería necesario realizar *firmware* específico para terminales que sí soportasen GPRS. Además habría que realizar modificaciones en las librerías que interpretan las tramas dentro del PC Linux para que reconociesen los nuevos formatos.

Una de las principales limitaciones de esta implementación es que únicamente permite acceder a los canales de comunicaciones permitidos a la tarjeta SIM y a la estación base a la que se encuentra el terminal conectado, siendo imposible interceptar las tramas de las estaciones base adyacentes del propio operador o de otro proveedor de servicios.

Se ha de tener en cuenta que el material utilizado para la realización del proyecto es fácilmente accesible y su coste es muy reducido en comparación a los analizadores comerciales que además, como se ha expuesto anteriormente, en su mayoría no consiguen las prestaciones que se alcanzan en nuestra implementación. Se detallan los componentes en la Tabla 6:

Ítem	Marca	Modelo	Función	Precio
Teléfono móvil GSM	Motorola	C118	Obtener las señales radio y decodificar la capa 1 del protocolo	23.80 €
Cable serie	Sysmocom	USB Serial	Enviar los datos desde el terminal móvil al PC	12.99 €
Tarjeta SIM	Cualquiera	SIM	Permitir el acceso a la red: puede ser una SIM personalizable o de un operador comercial	5 €
PC	Cualquiera	Cualquiera	Decodificar las capas superiores y representar los datos	Desde 200 €

Tabla 6: Modelos y precios de los equipos utilizados



Ilustración 62: Equipos utilizados para el analizador

En la Ilustración 62 pueden observarse los equipos utilizados para realizar el montaje del analizador de redes móviles GSM. El terminal aunque no posee grande especificaciones, es difícil de localizar debido a su antigüedad y que se encuentra

descatalogado por el fabricante. El PC por su parte no es necesario que tenga un hardware de última generación para poder soportar los servicios requeridos.

## Capítulo 5 – Despliegue de una celda GSM

## 5 Despliegue de una celda GSM

En este capítulo vamos a describir la implementación de un sistema GSM completo capaz de dar servicio a usuarios como si de un operador de telefonía se tratase. El objetivo será conseguir una implementación de los elementos mínimos necesarios que permitan, mediante el uso de terminales de telefonía móvil comerciales compatibles con el estándar GSM, conectarse a la red y acceder a los servicios básicos que ofrece la misma.

Existen varias alternativas para la implementación de una red con las características deseadas: establecimiento de una estación base libre, comunicación entre terminales GSM, mensajería SMS, gestión de llamadas y servicios añadidos e interconexión con redes externas. Se ha optado por el proyecto OpenBSC [23] de Osmocom basado en software libre ya que cuenta con las especificaciones necesarias. Las otras alternativas estudiadas se han desechado por los motivos que se detallan a continuación:

- Equipos hardware incompletos y excesivamente caros: en algunas soluciones no se ofrece un hardware completo sino que es necesario realizar un montaje complicado soldando los diferentes componentes. Además de aumentar la complejidad la durabilidad y el tamaño de la implementación resultaban excesivos. La elección final se compone de equipos estancos de fácil transporte que se interconectan mediante cableado de comunicaciones estándar. Otras implementaciones requerían equipos hardware comerciales que debido a su potencia y robustez para las condiciones de uso (elevado número de usuarios, ubicación en exteriores...) tenía un precio elevado que superaba las pretensiones del presente proyecto.
- Software propietario y licencias de uso: ya sea utilizando equipos comerciales o realizando el montaje de componentes discretos, muchas de las soluciones hacían uso de los mismos programas de control que utilizan las operadoras. Estos programas resultan muy sencillos de manejar y permiten un control más exhaustivo pero están protegidos por licencias que superan con creces el precio estimado para nuestra implementación.
- Falta de información y desarrollo: varias de las soluciones estudiadas no cuentan en la actualidad con un equipo de personas dedicadas al desarrollo. Por ello no se dispone de fuente de información para la solución de problemas o de los tutoriales adecuados para llevar a cabo nuestro proyecto.

### 5.1 OpenBSC de Osmocom

La plataforma OpenBSC persigue el objetivo de crear mediante software libre la implementación de los protocolos del estándar GSM/3GPP así como los componentes necesarios en las redes de comunicaciones que lo soportan. Además el proyecto OpenBSC es compatible con equipos hardware radiantes específicos para pequeños entornos. Estos cuentan con menor potencia y capacidad que los equipos utilizados por operadores y tienen un precio bastante más bajo. El software también es compatible con otras tecnologías que permiten la interconexión con otras redes externas y con otras implementaciones que añaden opciones extra de configuración. Dicho proyecto cuenta con una amplia comunidad de desarrolladores que se encargan de crear y corregir el código necesario para que el sistema funcione.

En estos momentos el software permite controlar una estación base y crear un red GSM a la que puedan conectarse terminales compatibles con el estándar. Además permite la interconexión de la red con centralitas telefónicas y con la RTC para que los terminales asociados a la red puedan comunicarse con otros terminales conectados a otras redes. Para ello se enrutan las llamadas a través de una centralita que permite gestionar las llamadas de la forma que se desee y tener el control absoluto sobre las comunicaciones. Aunque se expondrá en el siguiente capítulo, una de las partes en las que más se está avanzando, es en la adición de software para proporcionar servicio GPRS sobre el sistema implementado.

## 5.2 Implantación de un sistema GSM de bajo coste y software libre

El primer aspecto a realizar en el despliegue de una celda GSM es la implementación de interfaz radio que habilite la comunicación entre la BTS y el terminal móvil. La finalidad que perseguimos es la investigación de los entresijos del sistema GSM y poder experimentar diferentes configuraciones y variaciones de la red en un entorno de bajo coste. Posteriormente se fueron añadiendo los diferentes elementos que componen la red y controlan las comunicaciones como pueden ser la BSC y las bases de datos de usuario HLR y VLR.

Aunque hay varias opciones de uso dentro del proyecto, la más implementada y desarrollada se denomina *Network in the Box*. El software asociado contiene los componentes mínimos necesarios para desplegar una BSC capaz de controlar una BTS en tecnología GSM. Como se ha comentado antes, es posible implementar y configurar un red GSM en la que se pueda acceder a todos los servicios que proporcionan las redes convencionales gestionadas por los operadores de telefonía.

Aunque se trata de un proyecto de software libre, es necesario contar con hardware específico que soporte las comunicaciones sobre el interfaz radio. A pesar de disponer de soluciones abiertas para la implementación del interfaz radio, como OpenBTS [24], OpenBSC desde un principio se inclinó por emplear BTS comerciales. Con el tiempo han aparecido nuevas estaciones de menor coste, complejidad y tamaño y se ha modificado el software del proyecto para que éstas sean gestionable desde el mismo.

Pasaremos ahora a describir los componentes de la implementación. Aunque contienen diferentes componentes discretos, los principales son el hardware que implementa el interfaz radio (nanoBTS) y el software de control que se ejecuta sobre Unix (*osmo-nitb*)

### 5.2.1 nanoBTS

El hardware escogido para nuestra implementación es la nanoBTS 1800 proporcionado por el proveedor *ip.access* [25]. De tamaño reducido y con un coste permite dar soporte tanto para llamadas GSM como para comunicaciones de datos GRPS. El proveedor *ip.access* ofrece estaciones base con tecnología UMTS e incluso con LTE pero no se han contemplado para el presente proyecto debido a que no existen implementaciones software abiertas que permitan el control de las mismas.



Ilustración 63: nanoBTS GSM de ip.access

La nanoBTS proporciona el interfaz Abis sobre una conexión IP lo que facilita enormemente la conexión con un PC estándar mediante *sockets*. Las ráfagas de señalización utilizadas por el protocolo se encapsulan con una pequeña cabecera en diferentes sesiones TCP. En cambio, las ráfagas propias de los canales de tráfico se han de transportar dentro de segmentos UDP/RTC (*Real Time Protocol*) debido a que la temporización y los retardos son críticos para la calidad de las comunicaciones. Aunque el proyecto OpenBSC soporta la configuración de varias BTS sobre un sólo controlador BSC, se ha optado por la configuración de una sola BTS debido al elevado precio de cada una de las antenas necesarias, siendo con diferencia, el elemento más caro de la implementación. Además, la configuración multi-BTS no cuenta con el mismo soporte debido al limitado número de usuarios que se encuentran trabajando en su desarrollo y optimización. Para entornos de pruebas, objetivo del presente proyecto, una nanoBTS resulta suficiente para realizar ensayos y pruebas de configuración.



Ilustración 64: Equipos necesarios para realizar la implementación

Tal y como se observa en la Ilustración 64 son necesarios 4 equipos físicos para la implementación. La conexión física entre los equipos integrantes de la red se realiza mediante 100-Base-TX Ethernet. Es necesario utilizar alimentación PoE para que la BTS pueda operar. Para que todos los equipos puedan comunicarse deben encontrarse conectados a la misma red. Una vez conectada correctamente, la BTS obtiene una dirección IP válida de forma transparente mediante DHCP [26]. Tras esto, la estación escucha en el puerto 3006 paquetes broadcast UDP o A-bis-over-IP

mediante TCP. Empleando estos mecanismos el software *ipaccess-find* es capaz de identificar la estación base dentro de la red y obtener su dirección de red asignada.

### 5.2.2 osmo-nitb

La configuración escogida para realizar la implementación es denominada por el proyecto OpenBSC como *Network in the Box* y los elementos pueden observarse en la Ilustración 65. El software contiene los mecanismos de comunicación de la BSC y con la BTS mediante la interfaz Abis así como la implementación de las características mínimas de BSC, HLR y VLR para poder operar según el estándar GSM. Hay que destacar que no incluye ninguno de los elementos de conexión con el resto de la red, como pueden ser las MSC o el Gateway MSC de salida hacia otras redes. Posteriormente se describirán las alternativas que se han utilizado para poder implementar entidades que logren una función similar a los elementos troncales de red.

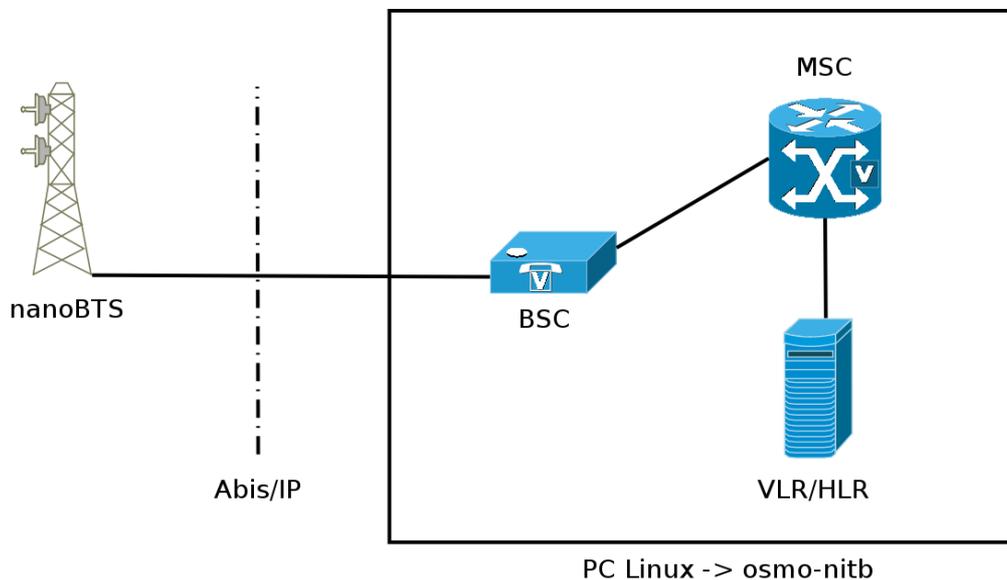


Ilustración 65: Arquitectura de la estación base basada en OpenBSC

Correctamente configurados los dos elementos, la estación base compatible y el software de control se consigue el despliegue de una celda GSM. Los diferentes componentes software se proporcionan para operar en entornos basados en Unix. Para ello, nuestro sistema necesita contar con una serie de librerías instaladas de las que dependen los programas de control. Entre ellos destaca la pila *mISDN* que implementa las librerías necesarias para que nuestro equipo entienda y utilice protocolos de las redes RDSI.

Aunque nuestra elección es la configuración más utilizada dentro del proyecto debido a que contiene todas las partes necesarias para operar la red como si se tratase de una red comercial cualquiera, su operativa no es exactamente igual en cuanto a distribución de equipos y la comunicación entre ellos. En este caso, se denomina BSC al conjunto de todos los elementos necesarios (BSC, HLR y VLR) que, aunque actúan como entidades diferenciadas, no siguen los mecanismos de comunicación no siguen, sino que emulan los de una red convencional. Por ello no es necesario tener los diferentes elementos por separado y establecer sesiones entre los mismos para que intercambien información sino que se ha recurrido a mecanismos más sencillos y en

su mayoría ya desarrollados para conseguir una red totalmente operativa. Esto reduce en gran medida la complejidad y nos permite ahora costes y capacidad de procesamiento.

Entre las opciones de configuración destacan la posibilidad de definir los de los *slot* temporales a emplear, la frecuencia de emisión, el identificador de celda... u otros más específicos como el tipo de acceso a la red (abierto, sólo usuarios autorizados o cerrada). Algunos de estos parámetros podrán ser modificados en tiempo real mientras que otros requerirán el reinicio del hardware y los programas controladores para que los cambios sean efectivos.

### 5.2.2.1 Implementación del HLR

Como se ha comentado anteriormente, la implementación de la red difiere en algunos aspectos con lo que el estándar GSM recomienda. La gestión de suscriptores es un claro ejemplo de ello dado que la funcionalidad se implementa usando bases de datos tradicionales, en lugar de emplear los mecanismos definidos en el estándar. Desde el proyecto OpenBSC, se ha empleado una base de datos *sqlite3* fácilmente configurable y accesible de forma directa por el software en el momento que sea necesario. La implementación disponible incluye capacidades adicionales como funciones que permiten el registro y gestión de las políticas de acceso y uso de la red por parte de los diferentes terminales de usuario.

Aunque existen tablas secundarias para la configuración y el almacenaje de parámetros, lo realmente necesario para poder dar servicio a los usuarios es la tabla de suscriptores (Tabla 7) almacenada en la base de datos *sqlite3*.

Nombre	Tipo	Descripción
imsi	Número simple	International Mobile Subscriber Identity. Se trata de un código único para cada tarjeta SIM que permite identificar al usuario dentro de cualquier red GSM/3G.
name	Texto	Nombre del abonado. Se utiliza para diferenciar a cada abonado, no es relevante ya que es un parámetros meramente informativo.
extension	Texto simple	Extensión. Identifica al abonado dentro de la red. Es el número que ha de marcarse para realizar una llamada al terminal y el que aparecerá en el terminal llamado.
authorized	Entero no nulo Valor por defecto '0'	Autorización. Con el valor '1' indicamos, en caso de que el acceso esté cerrado, que el abonado sea aceptado en la red cuando intente el acceso.
tmsi	Texto simple	Temporary Mobile Subscriber Identity. Es un identificador temporal que asigna el VLR al móvil cuando se conecta. Sólo tiene sentido dentro de un determinado área.
lac	Entero no nulo Valor por defecto '0'	Location Area Code. Se trata del código de área del suscriptor necesario para enrutar las llamadas entrantes.

Tabla 7: Parámetros en la base de datos de abonados

Si bien la base de datos de gestión se puede manejar accediendo y operando directamente sobre ella, se recomienda emplear las funcionalidades que ofrece *osmonitb* para la gestión de ésta, lo que asegura la actualización correcta de los diferentes campos ya que modificando la base de datos manualmente cualquier error de escritura puede provocar fallos en el funcionamiento del software.

Todo el software se instala sobre un entorno Unix y no es necesario contar con ninguna librería adicional. Los requerimientos hardware del PC, aunque no se especifican, no son críticos puesto que los procesos no consumen apenas recursos. Cualquier PC que incluya conexión WiFi o Ethernet debería bastar. El único limitante es la arquitectura del sistema operativo ya que aunque los procesadores pueden ejecutar sistemas de 32 o 64 bits, las librerías que instala OpenBSC no son compatibles con estos últimos.

### 5.2.3 Uso y operación de nuestra estación base

Una vez que el software ha sido instalado correctamente ya se puede proceder a poner en marcha la estación base. El primer paso es conocer las direcciones IP de los equipos de comunicaciones (PC y nanoBTS). Ambos obtienen su dirección de red mediante DHCP. Por ello es necesario configurar dentro del switch el direccionamiento estático. Dicha configuración se realiza conociendo la dirección MAC del dispositivo y asociándola a la IP que deseamos asignar al equipo. Para la nanoBTS se utilizará el programa *ipaccess-find* que envía un paquete broadcast dentro de la red local interrogando a los dispositivos para conocer las direcciones de red de la nanoBTS. En el caso del PC ejecutamos el comando *ifconfig* en el terminal de Linux y obtendremos la información necesaria. Se han configurado las siguientes IP's estáticas según indica la tabla Tabla 8.

Equipo	Dirección IP asignada
nanoBTS	192.168.100.2
PC Linux	192.168.100.50

Tabla 8: Direcciones de red de los equipos

Seguidamente se configurarán, mediante el comando *ipaccess-config*, los parámetros básicos de la BTS, que serán alojados en su memoria NVRAM y fijarán la configuración de inicio. Es necesario destacar que la mayoría de configuración realizadas cuando la BTS está en ejecución no se guardarán como configuración por defecto a no ser que se realice el volcado de la actual a la memoria persistente. Esto provoca que al reiniciar la estación base, se cargará la configuración de inicio y no la que hemos modificado. Se indicarán como parámetros dentro del programa la IP de la nanoBTS con la que contactar, la dirección IP de la BSC que debe controlar la antena y el nombre que se le desea asignar al dispositivo. Además pueden introducirse diferentes parámetros para testear los canales y enlaces que está emitiendo el dispositivo y la ocupación de los mismos. Las medidas que se devuelvan facilitarán la identificación de las frecuencias libre o aquellas en las que se recibe señal más débil, de forma que se asigne un canal a nuestro equipo que no interfiera con los ya ocupados.

El programa de inicio de la estación base, y por tanto, el que conseguirá que el equipo comience a emitir señales GSM y el sistema se ponga en funcionamiento es *osmonitb*. Dispone de un gran abanico de parámetros de configuración. La configuración más básica debe incluir entre otros los parámetros enumerados en la Tabla 9.

Parámetro	Valor	Detalle
network country code	214	Código del territorio español
mobile network code	29	Código de red no utilizado
short name	OpenBSC	Nombre corto de la red
long name	OpenBSC	Nombre largo de la red
auth policy	closed	Sólo admitidos usuarios registrados
type	nanobts	Tipo de BTS
band	DCS1800	Banda GSM en la que opera la red
cell_identity	425	Identificador de celda
location_area_code	8001	Código de área para <i>roaming</i>
ms max power	15	Límite de potencia para restringir el alcance

Tabla 9: Parámetros clave de configuración del software osmo-nitb

Los valores por defecto se configuran mediante el fichero *openbsc.cfg* [Apéndice1]. Una vez que la base se encuentra arrancada algunos de ellos pueden modificarse en tiempo real y ser guardados como configuración base. Otros sin embargo, requieren un reinicio de los equipos para hacerse efectivos.

Dado que se busca no interferir con los sistemas comerciales, se ha limitado la potencia de transmisión restringiendo el alcance de la estación base al entorno del laboratorio, lo que unido a que los terminales no puedan registrarse si no están dados de alta, evita riesgo de interferir con los móviles que operan en las redes GSM convencionales. Por otro lado se han configurado los *slots* temporales de emisión según se representa en la Tabla 10:

Canales	Distribución en <i>slots</i>
Canales de tráfico: TCH/F	2, 3, 4, 5,6 y 7
Canales de control y señalización: CCCH+SDCCH4	0
Canales de señalización: SDCCH8	1

Tabla 10: Distribución de canales en la nanoBTS

Configuradas correctamente tanto la estación base como el software BSC se puede proceder a poner en marcha la celda GSM con el siguiente comando:

```
/opt/openbsc/bin$ sudo ./osmo-nitb
```

Tras la ejecución del comando, la consola muestra unas líneas similares a la Ilustración 66 donde podemos comprobar los parámetros de configuración. Teniendo ya el sistema en funcionamiento, el último paso antes de comenzar su utilización es asociar terminales móviles con los que poder operar. Como se indicó con anterioridad, los terminales deben estar autorizados dentro de la base de datos de abonados para que el equipo permita su acceso a la red de la forma que se indicó en el apartado anterior. Fijándonos en la forma de proceder a la hora de registrar nuestro terminal se distinguen dos casos:

- SIM configurada con los mismos parámetros: En este caso, al coincidir el código del país y el código de operador configurados en la nanoBTS y el terminal, éste se asociará directamente siempre y cuando no exista otra antena del mismo operador que ofrezca una señal más potente.
- SIM configurada con diferentes parámetros: Si la tarjeta difiere en alguno de los dos identificadores debemos acceder a las opciones del terminal y seleccionar de forma manual el operador al que queremos conectarnos.

```

<0019> ipaccess.c:842 enabling ipaccess BSC mode
DB: Database initialized.
DB: Database prepared.
<0007> sms_queue.c:232 Attempting to send 20 SMS
<0019> ipa.c:319 accept()ed new link from 192.168.100.2 to port 3002
Failure Event Report Type=communication failure Severity=critical failure Probable cause= 0
3 03 11 Additional Text=
<0019> ipa.c:319 accept()ed new link from 192.168.100.2 to port 3003
<0004> bsc_init.c:281 bootstrapping RSL for BTS/TRX (0/0) on ARFCN 770 using MCC=214 MNC=29
LAC=8001 CID=425 BSIC=63 TSC=7

```

Ilustración 66: Consola de salida al inicio de osmo-nitb

El siguiente paso es asociar los móviles en la red. Cuando se utiliza un terminal con una tarjeta SIM en la que no está configurada nuestra red entre las preferidas es necesario intentar una conexión manual. Tras un primer intento, como hemos configurado que sólo se admitan terminales dados de alta, el intento es fallido. Pero este procedimiento hace que queden registrados en la base de datos de la entidad que actúa como HLR de nuestra red. A diferencia de las redes comerciales, no se realiza un intercambio de claves ni una autenticación de los terminales dentro de la red ya que ésta por simplicidad está desactivada. Esto se consigue gracias a que los terminales móviles son pasivos y la estación base le obliga a no autenticarse. Para el caso que nos ocupa se ha utilizado una tarjeta SIM estándar de un operador convencional. Mediante las opciones del terminal de telefonía se ha configurado de modo que no intente conectarse de manera automática a la red que tiene como favorita. Posteriormente se realiza un escaneo de las redes disponibles y se escoge la que posee el identificador que hemos configurado dentro de nuestra celda. Se trata de una etiqueta numérica MCC+MNC debido a que el nombre del proveedor, que aparece normalmente en el terminal, ha de estar preconfigurado en la tarjeta SIM. En la Ilustración 67 podemos observar la pantalla de un terminal telefónico con el menú de selección de red.



Ilustración 67: Selección manual de red en terminal GSM

Una vez realizado este paso comprobaremos que el terminal aún no es capaz de asociarse a nuestra red por lo que necesitamos darle autorización dentro de la base de datos. Debemos modificar el registro de la base de datos para autorizarlo. Para ello deben cambiarse los parámetros en el archivo con el programa de gestión de base de datos *sqlite3*. Mediante la secuencia siguiente podemos listar los parámetros de los terminales que la estación base ha detectado:

```

$ sudo sqlite3 hlr.sqlite3
sqlite> select * from subscriber;
1|2013-03-13 17:08:14|2013-03-13
17:08:14|214039582124729||40884|0||0

```

El programa gestor de la base de datos nos muestra esta línea donde se ven los datos comentados anteriormente. Además se ofrece la fecha de la primera conexión y de la última para facilitar la identificación de cada uno de los móviles con los que vamos a operar y poder autorizar al que deseamos. Recordemos que el software de control también toma funciones de MSC, es decir, se encarga de enrutar las llamadas y ejercer de centralita de la red. Por esto, también es necesario proporcionar los datos del abonado a fin de identificarle dentro de la red. Vamos a cambiar su número de extensión (que actúa como número telefónico GSM), su nombre y lo autorizaremos para que pueda asociarse a la red:

```
sqlite> update Subscriber set authorized=1 where
imsi=214039582124729;
sqlite> update Subscriber set name='uno' where
imsi=214039582124729;
sqlite> update Subscriber set extension=2003 where
imsi=214039582124729;
sqlite> select * from subscriber;
1|2013-03-13 17:08:14|2013-03-13
17:08:14|214039582124729|uno|2003|1||0
```

Volvemos a realizar la elección manual de red. Cuando el móvil indique el nombre de operador que hemos asignado a nuestra estación base y comprobemos que tenemos cobertura, ya se puede operar dentro de la red. Su número será el establecido en el paso anterior y se podrá utilizar para contactar con el terminal mediante una llamada de voz o bien mediante un SMS. El problema en este momento es que nos encontramos con una red aislada en la que sólo podemos comunicarnos con terminales que estén campeando en la misma celda que nuestro terminal. Más adelante con la utilización de una centralita de voz que nos permitirá además realizar configuraciones más avanzadas, se podrá establecer la comunicación entre varios terminales dentro de la misma celda.



Ilustración 68: Terminal asociado a nuestra estación base

En la Ilustración 68 comprobamos que efectivamente el terminal está asociado a nuestra estación base y tiene cobertura. Hay que añadir, que además de las opciones y servicios propios de la red GSM, con la infraestructura mostrada es posible realizar nuevas operaciones restringidas al administrador de la red. A continuación se expondrán diversas operaciones realizadas desde la consola de control del software *osmo-nitb* para comprobar el funcionamiento y las opciones de las que dispone la herramienta.

#### 5.2.4 Operaciones disponibles en nuestra estación base

El software disponible en OpenBSC permite acceder al estado instantáneo de la red, pudiendo obtener información sobre los suscriptores que se encuentran conectados o que tienen autorización, así como ver los parámetros de la red y las medidas periódicas que se realizan. Además nos permite realizar modificaciones en tiempo real sobre las configuraciones de los abonados o sobre las características de la red. El montaje implementa también la posibilidad de enviar notificaciones a todos los dispositivos conectados mediante operaciones tipo *broadcast*.

El acceso al interfaz de interacción es proporcionado por el programa *osmo-nitb* y se realiza mediante *telnet* estando, por defecto, el servidor disponible en el puerto 4242. A continuación se describen algunas de las funcionalidades más relevantes a las que se puede acceder mediante esta consola.

### 5.2.4.1 Información sobre el estado de la red

El primer comando para obtener información sobre los parámetros y la configuración de la red GSM es *show network*. La información mostrada por el comando puede verse en la Ilustración 69.

```
OpenBSC# show network
BSC is on Country Code 214, Network Code 29 and has 1 BTS
Long network name: 'OpenBSC'
Short network name: 'OpenBSC'
Authentication policy: closed
Location updating reject cause: 13
Encryption: A5/0
NECI (TCH/H): 1
Use TCH for Paging any: 0
RRLP Mode: none
MM Info: On
Handover: Off
Current Channel Load:
  CCCH+SDCCH4:  0% (0/4)
  TCH/F:        0% (0/4)
  SDCCH8:       0% (0/8)
```

Ilustración 69: Estado de la red GSM

Además de los parámetros ya configurados, se pueden observar gracias al comando anterior cómo el *handover* está desactivado debido a que únicamente hay una estación base configurada. En este caso no cabría hablar de traspaso entre celdas. También podemos ver que se muestra la ocupación actual de los canales de comunicaciones.

Otro comando similar pero que ofrece información sobre el estado de una BTS concreta es *show bts* cuya salida debería ofrecer un resultado similar al mostrado en la Ilustración 70.

```
OpenBSC# show bts
BTS 0 is of nanobts type in band DCS1800, has CI 425 LAC 8001, BSIC 63, TSC 7 and 1 TRX
Description: (null)
MS Max power: 15 dBm
Minimum Rx Level for Access: -110 dBm
Cell Reselection Hysteresis: 4 dBm
RACH TX-Integer: 9
RACH Max transmissions: 7
System Information present: 0x0000087e, static: 0x00000000
  Unit ID: 1800/0/0, OML Stream ID 0xff
  NM State: Oper 'Enabled', Admin 2, Avail 'OK'
  Site Mgr NM State: Oper 'Enabled', Admin 0, Avail 'OK'
  Paging: 0 pending requests, 20 free slots
```

Ilustración 70: Información sobre la BTS

En este caso se amplía la información y se pueden comprobar los niveles de potencia de recepción y emisión así como operaciones pendientes, enlaces de datos o estado de los protocolos de señalización. También son útiles comandos *show trx* (Ilustración 71) y *show timeslot* que nos indican el estado de cada una de las frecuencias de emisión y el de sus *slots* temporales respectivamente. Puede observarse por ejemplo la potencia efectiva emitida por la estación base.

```
OpenBSC# show trx
TRX 0 of BTS 0 is on ARFCN 770
Description: (null)
RF Nominal Power: 23 dBm, reduced by 20 dB, resulting BS power: 3 dBm
```

Ilustración 71: información sobre el TRX

```
OpenBSC# show statistics
Channel Requests      : 2 total, 0 no channel
Channel Failures     : 0 rf_failures, 1 rll failures
Paging                : 0 attempted, 0 complete, 0 expired
BTS failures         : 0 OML, 0 RSL
Channel Requests     : 2 total, 0 no channel
Location Update      : 1 attach, 1 normal, 0 periodic
IMSI Detach Indications : 0
Location Update Response: 2 accept, 0 reject
Handover              : 0 attempted, 0 no_channel, 0 timeout, 0 completed, 0 failed
SMS MO                : 0 submitted, 0 no receiver
SMS MT                : 0 delivered, 0 no memory, 0 other error
MO Calls              : 0 setup, 0 connect ack
MT Calls              : 0 setup, 0 connect
```

Ilustración 72: Estadísticas referentes a la red

Por último, es posible ver una serie de estadísticas mediante el comando *show statistics*. Las peticiones de canales, los fallos de las diferentes partes, las asociaciones, las llamadas y los mensajes gestionados por la red tal y como se muestra en la Ilustración 72.

#### 5.2.4.2 Información y operaciones sobre los terminales asociados

Para ver la información sobre los terminales autorizados en nuestra red, utilizaremos el comando *show subscriber* seguido de *extension*, *tmsi*, *imsi* o *id* según el criterio de selección que queramos deseemos. El terminal mostrará la información del abonado seleccionado. El resultado será el mostrado en la Ilustración 73 pero con los datos del abonado seleccionado.

```
OpenBSC# show subscriber id 4
ID: 4, Authorized: 1
Name: 'uno'
Extension: 2003
LAC: 8001/0x1f41
IMSI: 214039582124729
TMSI: 3B41C099
Pending: 0
Use count: 1
```

Ilustración 73: información del abonado con ID 4

Como se comentó ha citado anteriormente, es posible modificar la base de datos de usuarios desde la consola sin necesidad de modificar el archivo *sqlite3*. Para ello debemos introducir el comando *subscriber* seguido de cualquiera de los identificadores comentados en el párrafo anterior. Tras esto podremos cambiar alguno de los identificadores, eliminar las operaciones pendientes, autorizar al terminal en la red, desactivar los servicios de llamadas o SMS, o forzar el envío de un SMS al abonado. Con esta última opción podrían configurarse mensajes de bienvenida a la red y otros servicios de alerta en nuestra estación base, lo cuál son opciones de valor añadido que podrían implementarse de forma sencilla.

```

OpenBSC# subscriber id 1
  sms          SMS Operations
  silent-sms   Silent SMS Operation
  silent-call  Silent call operation
  ussd-notify  USSD Notify
  update      Update the subscriber data from the dabase.
  name        Set the name of the subscriber
  extension   Set the extension (phone number) of the subscriber
  authorized  (De-)Authorize subscriber in HLR
  a3a8        Set a3a8 parameters for the subscriber
  clear-requests Clear the paging requests for this subscriber
  show-pending Clear the paging requests for this subscriber
  kick-pending Clear the paging requests for this subscriber

```

Ilustración 74: Operaciones sobre la base de datos de usuarios

### 5.2.4.3 Operaciones sobre la estación base

Al igual que en el apartado anterior, es posible realizar la configuración de los parámetros de la estación base desde la consola de control. Por un lado se pueden configurar los canales de cada *slot* temporal mediante el siguiente comando:

```
OpenBSC# bts 0 trx 0 timeslot X
```

Donde X es el número de *timeslot* que deseamos modificar. Como sólo tenemos una estación base ésta será la número '0', como también lo será el identificador asignado al transmisor que sólo emite en una frecuencia. Aunque con la configuración por defecto es posible operar correctamente sin ninguna modificación, puede modificarse la distribución de canales dentro de los *slot* temporales. En las implementaciones reales hay varios tipos de patrones según la demanda de servicios y los clientes que se encuentren registrados en la estación base.

Se ofrece la posibilidad de realizar la configuración de otros múltiples parámetros de emisión, etc... mediante el comando *configure terminal* dentro del submenú *network*, tal como se refleja en la Ilustración 75.

```

OpenBSC(network)#
  help          Description of the interactive help system
  list         Print command list
  write        Write running configuration to memory, network, or terminal
  show        Show running system information
  exit        Exit current mode and down to previous mode
  end         End current mode and change to enable mode.
  network     Set the GSM network country code
  mobile      Set the GSM mobile network code
  short       Set the short GSM network name
  long        Set the long GSM network name
  auth        Authentication (not cryptographic)
  location    Set the reject cause of location updating reject
  encryption  Encryption options
  neci        New Establish Cause Indication
  rrlp        Radio Resource Location Protocol
  mm          Whether to send MM INFO after LOC UPD ACCEPT
  handover    Handover Options
  timer       Configure GSM Timers
  dtx-used    Enable the usage of DTX.
  subscriber-keep-in-ram Keep unused subscribers in RAM.
  paging      Assign a TCH when receiving a Paging Any request
  bts        Select a BTS to configure

```

Ilustración 75: Opciones de configuración de la estación base

Aunque únicamente se puede acceder a la consola con el programa en ejecución, es necesario reiniciar el programa *osmo-nitb* para que los cambios en la configuración de la nanoBTS tengan efecto ya que éstos se almacenan en el software pero el hardware se configura al inicio y no puede ser modificado en tiempo real. No ocurre así con los cambios realizados en el HLR que se aplicarán de forma inmediata ya que se trata de una base de datos independiente y que es consultada por el programa que controla la estación base únicamente cuando es necesario.

### 5.2.5 Servicios de voz y SMS

Para comprobar el funcionamiento de la estación base, se han configurado dos móviles dentro de la red utilizando tarjetas de los operadores comerciales. Se han configurado dos terminales con los parámetros mostrados en la Tabla 11. Recordemos que la configuración se realiza dentro de la base de datos *sqlite3* que realiza funciones equivalentes al HLR del estándar GSM.

SIM	IMSI	Nombre	Extensión
Orange	214039582124729	orange mobile	2003
MoviStar	214075531908988	movistar mobile	2004

Tabla 11: Datos de abonados en el HLR

Una vez que se autoriza a ambos para poder utilizar la red, es hora de probar los servicios. Se ha enviado un SMS desde la extensión 2004 a la 2003 y también se ha realizado una llamada. Tal y como se observa en la Ilustración 76, ambos servicios funcionan satisfactoriamente.



Ilustración 76: Llamada (izquierda) y SMS (derecha) entrantes

Una vez que se ha implementado una red en la que pueden registrarse terminales GSM y comunicarse entre ellos, bien mediante llamadas de voz o por el servicio SMS, se añadirá una centralita que permita configuraciones avanzadas en la gestión de las llamadas y se realizará la conexión con otras redes externas. El resumen del equipamiento y los costes derivados se realizará en el capítulo siguiente para tener una visión completa de la implementación.

## Capítulo 6 – Integración de celda GSM con centralita VOIP y la RTC

## 6 Integración de celda GSM con centralita VOIP y la RTC

Se ha mostrado en el capítulo anterior una implementación capaz de gestionar llamadas de voz y SMS mediante el estándar GSM. En el presente capítulo se añadirán dos prestaciones nuevas a la estación base partiendo de lo anterior: integración con centralita IP para gestión avanzada de los servicios de voz e interconexión con la red telefónica conmutada. Por último se expondrá un ejemplo de ataque contra la seguridad del estándar GSM utilizando la implementación realizada.

### 6.1 Integración con centralita de VoIP

Aunque la red GSM implementada es totalmente operativa, se ha comentado con anterioridad que no es posible la comunicación con equipos que se encuentren fuera de la misma. Además el software OpenBSC tampoco permite configuraciones avanzadas como pueden ser la restricción de llamadas, buzón de voz, desvíos... Para poder acceder a estos servicios debe recurrirse a una PBX o centralita de comunicaciones de voz y configurar la misma para que soporte servicios adicionales.

Para incrementar las prestaciones del despliegue realizando en este proyecto, se ha optado por emplear Asterisk [27] como soporte PBX. Esta decisión se debe a que presenta la mejor compatibilidad trabajando con OpenBSC de todas las opciones. Asterisk es un software que comenzó a desarrollarse en el año 1999 para ofrecer los servicios de una centralita. La disposición de los elementos dentro de la infraestructura queda reflejada en la Ilustración 77.

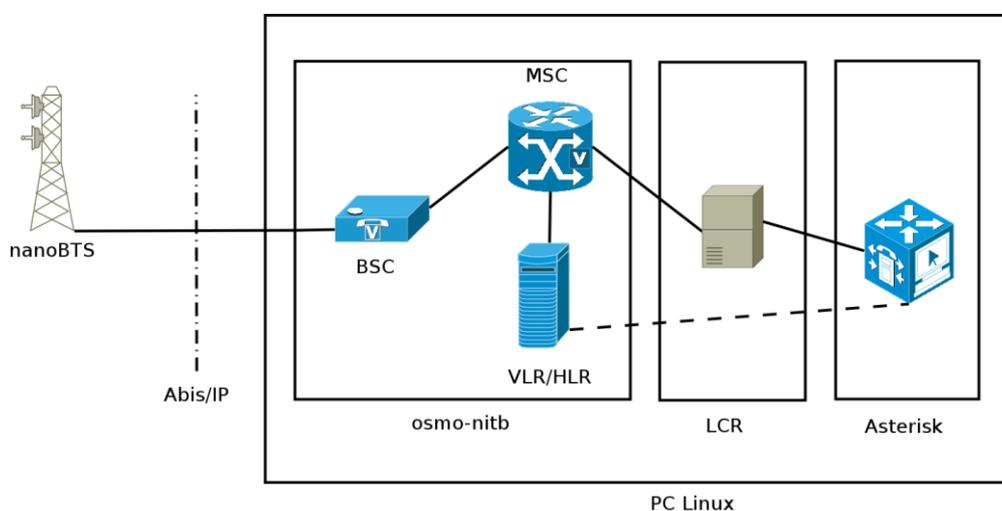


Ilustración 77: Esquema de interconexión de los diferentes elementos

Las funciones que pueden implementarse dentro de la PBX son:

- Conexión de terminales telefónicos VoIP
- Conexión con proveedores IP o líneas RDSI
- Configuración de servicios adicionales: llamada en espera, desvíos, buzón de voz...

Aunque el sistema de centralita opera enteramente con Voz sobre IP, es posible mediante adaptadores conectar al sistema extensiones o primarios analógicos.

En la actualidad existen multitud de versiones de Asterisk así como distribuciones Linux específicas preconfiguradas con este sistema. Para este proyecto hemos escogido la versión 1.8.6.0.

La conexión entre OpenBSC y Asterisk se realiza mediante el software LCR [28]. El cometido principal de este software es proporcionar una centralita de voz RDSI dentro de un sistema operativo Linux. En este sentido los integradores de OpenBSC han aprovechado la especificación y utilización del *backbone* RDSI del estándar GSM. LCR incluye a su vez los drivers de interconexión con Asterisk lo que facilita la integración.

Desde el proyecto OpenBSC se ha creado un canal denominado *MNCC socket* que transporta la información proveniente de la estación base hacia el LCR, quien dirige dicho flujo a la centralita Asterisk.

### 6.1.1 Instalación y configuración del software necesario

Como ya contamos con una versión de OpenBSC operativa debemos instalar únicamente LCR y Asterisk. Asterisk funciona como PBX dentro de una red IP por sí mismo sin necesidad de añadidos, mientras que para operar a través de LCR es necesario tener instalados los módulos del *kernel* *mISDN* y *mISDN\_user*, usualmente disponibles en las distribuciones actuales del sistema operativo Linux.

El proceso de instalación y configuración se describe a continuación. La instalación de Asterisk se puede realizar empleando los repositorios software de la distribución:

```
$ sudo apt-get install asterisk
```

Por el contrario, el LCR usualmente no está incluido en la mayoría de distribuciones Linux y es necesario realizar la compilación a partir del código fuente obtenido desde el repositorio *git*.

```
$ git clone git://git.misdn.org/lcr.git/
$ cd ../../lcr
$ ln -s ../libosmocore/ .
$ ln -s ../openbsc/openbsc/ .
$ sh autogen.sh
$ ./configure --prefix=/opt --with-asterisk --with-gsm-bs
$ make
$ sudo make install
```

Para simplificar la instalación de las diferentes librerías se recomienda realizar todos los procesos sobre el mismo path de instalación empleado para OpenBSC. Es importante destacar las opciones *--with-asterisk* y *--with-gsm-bs* para que se realice la configuración de LCR adecuada para la interacción por un lado con Asterisk y con OpenBSC por el otro. Por último debe copiarse como módulo de Asterisk la librería *chan\_lcr* necesario para la conexión.

```
$ cp chan_lcr.so /usr/lib/asterisk/modules/
```

Para automatizar la carga del módulo en cada arranque se añadirá la siguiente línea en el archivo */etc/modules.conf*:

```
load => chan_lcr.so
```

También es posible automatizar la carga de los módulos de kernel instalados anteriormente añadiendo al archivo `/etc/modules` las siguientes líneas:

```
mISDN_core
mISDN_dsp
mISDN_l1loop pri=1 nchannel=30
```

Es necesario activar también la disponibilidad del módulo LCR en Asterisk a través de la configuración del fichero `/usr/local/lcr/options.conf` del mismo modo que se hizo en el otro extremo cuando se añadió el módulo de Asterisk.

```
socketuser asterisk
socketgroup asterisk
```

Ahora sólo queda configurar la centralita Asterisk para que se conecte a LCR y de servicio a las extensiones de OpenBSC y a otras extensiones VoIP.

## 6.1.2 Configuración básica de Asterisk

La configuración necesaria de la centralita Asterisk supone la modificación de las opciones de configuración alojadas en los archivos `sip.conf` [Apéndice2] y `extensions.conf` [Apéndice3]. En el primero hemos definido una serie de extensiones VoIP que se conectan mediante protocolo SIP a nuestra centralita. El segundo archivo es considerado el archivo principal de Asterisk ya que define el enrutamiento y el tratamiento de las llamadas que gestiona la PBX. Veamos cómo funcionan ambos ficheros.

### 6.1.2.1 sip.conf

Se ha configurado una extensión SIP para comprobar que efectivamente las llamadas son tratadas por la centralita. Bastaría con utilizar cualquier *softphone* compatible con el protocolo SIP para poder realizar llamadas a teléfonos de nuestra red GSM.

```
[1002]
type=friend
context=btsctrl
host=dynamic
secret=1002
nat=no
```

El número y nombre de la extensión es el 1002. Además se le ha indicado que sea de tipo *friend* para que pueda enviar y recibir llamadas. Otros tipos serían *user* que sólo podría recibir llamadas o *peer* que sólo podría realizarlas. Como se verá a continuación, la extensión utiliza el contexto *btsctrl* para dirigir sus llamadas. *host=dynamic* permite conectarse desde cualquier IP introduciendo el usuario 1002 y la contraseña que también se ha configurado en *secret*. Por último indicamos *nat=no* debido a que nos encontramos en un entorno local en el que no es necesario realizar traducción de direcciones.

### 6.1.2.2 extensions.conf

Para diferenciar grupos de usuarios a la hora de enrutar las llamadas, Asterisk utiliza lo que se denominan contextos. Estos contextos permiten realizar una serie de acciones que se ejecutan de forma secuencial cuando se recibe una llamada. La ejecución de las mismas se realiza de forma secuencial según han sido escritas en el archivo de configuración. A continuación se muestra las órdenes utilizadas:

```
[btsctrl]
exten => _20XX,1,Answer
exten => _20XX,n,Dial(LCR/GSM/${EXTEN},20)
exten => _20XX,n,Hangup

exten => _10XX,1,Answer
exten => _10XX,n,Dial(SIP/${EXTEN},20)
exten => _10XX,n,Hangup
```

El símbolo ‘\_’ significa que no se especifica el número exacto sino que la orden puede ejecutarse en varios números con cifras en común. En nuestro caso tenemos por un lado las extensiones asignadas a móviles de la forma 20XX (que se encuentran definidas en el LCR) y las de extensiones SIP de la forma 10XX. El contexto *btsctrl* agrupa las políticas que definen que cuando se marquen números dentro de esas extensiones, la centralita atienda esas llamadas y, según su naturaleza envíe la llamada a las extensiones SIP o a las GSM/LCR (las configuradas en LCR). Con *\${EXTEN}* se enviará el número marcado completo y el parámetro 20 significa que tras 20 segundos deseche la llamada si el destinatario no ha descolgado. La última orden es para que no se queden los canales abiertos cuando se terminal la llamada.

### 6.1.2.3 routing.conf

Para esta configuración en conjunción con el LCR y la estación base, es necesario configurar además el archivo de enrutamiento del LCR. El archivo no se encuentra en la configuración de Asterisk sino en la del LCR en el path */usr/local/lcr/routing.conf* [Apéndice4]:

```
[main]
interface=GSM : remote application=asterisk
context=btsctrl
```

De esta manera relacionamos el interfaz RDSI que llega al LCR desde OpenBSC (interface=GSM) hacia el contexto *btsctrl* de Asterisk. Dicho interfaz se encuentra configurado en el archivo */usr/local/lcr/interface.conf* [Apéndice5] y viene definido por defecto en la instalación. Únicamente incluye la línea *gsm-bs* que significa operación en modo estación base GSM.

### 6.1.3 Uso y operación del sistema a través de la centralita Asterisk

Para comprobar que el sistema funciona correctamente se emplea un *softphone* asociado a la centralita con el usuario SIP que hemos definido. Hemos elegido el software *Telephone* [29] para Mac Os X. En la Ilustración 78 se observa el formulario donde se configura un usuario con los parámetros deseados.

Description:	Pruebas Asterisk 2
Full Name:	
Domain:	192.168.100.50
User Name:	1002
Password:	****

Ilustración 78: Configuración usuario SIP

El usuario está asociado al dominio de la máquina que ejecuta Asterisk, por lo que como servidor o *proxy* SIP se debe configurar la dirección del servidor Asterisk.

En esta ocasión, antes de arrancar el programa *osmo-nitb* es necesario arrancar LCR y Asterisk. Se añadirá la opción *-m* a la hora de ejecutar *osmo-nitb* para indicar la activación del canal MNCC para comunicarse con LCR:

```
$ sudo /opt/openbsc/bin/osmo-nitb -m
```

```
** LCR Version 1.10
000000 DEBUG (in getrulesetbyname() line 1871): ruleset main found.
000000 DEBUG (in mISDNloop_open() line 36): Open external interface of loopback.
000000 DEBUG (in mISDNport_open() line 2388): Port has 30 b-channels.
000000 DEBUG (in mISDNport_open() line 2409): using 'mISDN_dsp.o' module
000000 TRACE 14.03.13 18:41:36.970 CH: PORT (open) port 1 mode network channels 30
000000 ERROR (in mncc_socket_retry_cb() line 1102): Could not connect to MNCC socket /tmp/bsc_mncc, retrying in 5 seconds
LCR 1.10 started, waiting for calls...
000000 TRACE 14.03.13 18:41:37.066 --: LCR 1.10 started, waiting for calls...
000000 TRACE 14.03.13 18:41:39.002 --: REMOTE APP registers app name=asterisk
000000 DEBUG (in mncc_socket_retry_cb() line 1106): Connected to MNCC socket /tmp/bsc_mncc!
```

Ilustración 79: Arranque del programa LCR

Tal y como se puede comprobar en la Ilustración 79, en un primer momento se indica que no es posible abrir el *socket MNCC*. Esto se debe a que la estación base aún no se encuentra operativa debido a que aún está arrancando *osmo-nitb*. Después se observa que la conexión con Asterisk es correcta y que ahora sí, se ha establecido el canal de conexión con la estación base OpenBSC. La consola de ejecución del programa *osmo-nitb* también muestra que se ha realizado la conexión con un gestor de llamadas externo (Ilustración 80).

```
<0006> mncc_sock.c:274 MNCC Socket has connection with external call control application
```

Ilustración 80: Arranque osmo-nitb con socket MNCC

Ahora ya es posible comprobar el funcionamiento dado que todos los sistemas están operativos. El *softphone* indica que hay conexión con la centralita y los móviles cuentan con cobertura de nuestra estación base. Desde uno de los teléfonos configurados en el HLR se realiza una llamada a la extensión SIP 1002, extensión configurada fuera de la red GSM. Se comprueba (Ilustración 81) que efectivamente funciona la comunicación de forma adecuada. Se realiza otra prueba en sentido contrario con idéntico resultado.

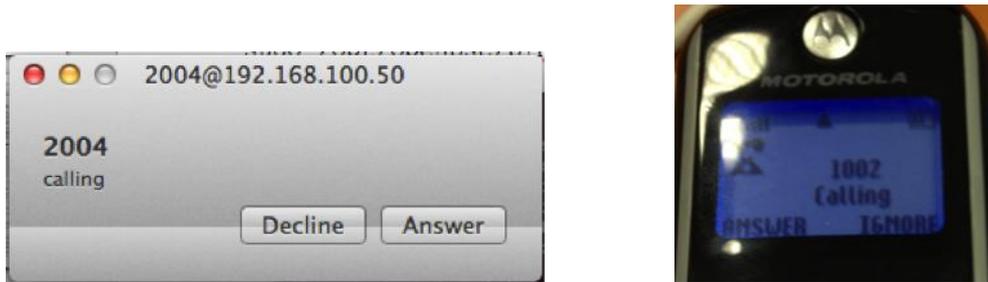


Ilustración 81: Llamada recibida en extensión SIP(izquierda) y móvil(derecha)

## 6.2 Conexión con la RTC

Para dotar a la red GSM implementada de conectividad con redes de telefonía (tanto fijas como móviles) no sólo necesitamos realizar configuraciones a nivel software sino que también hay requisitos que sólo pueden implementarse con elementos hardware. Aunque hay 2 opciones diferentes, siempre debemos disponer de un PTR de telefonía para poder enviar los datos bien a la red Internet como datos de voz sobre IP o a la RTC de los operadores comerciales. Es necesario por tanto disponer bien de una línea ADSL o de una línea telefónica analógica convencional. La Ilustración 82 ilustra perfectamente los elementos y su interconexión dentro de la red.

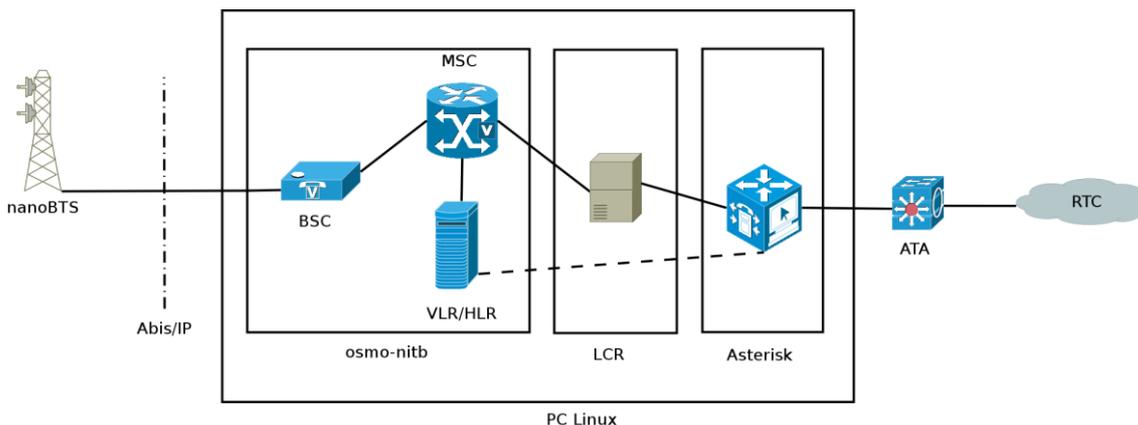


Ilustración 82: Esquema del sistema GSM completo con la salida a la RTC

La primera de las opciones implica contratar un servicio de VoIP con cualquiera de los operadores que ofrecen dicho servicio. Uno de los más famosos son MegaVoip [30] o EasyVoip [31] que ofrecen por una parte sus propias aplicaciones pero también permiten configurar otras aplicaciones o centralitas VoIP. La configuración para interconectar la línea que nos proporcionen será la que el operador nos indique. El requisito en este caso será contar además con conexión a Internet para poder enviar nuestras peticiones al servidor VoIP que hayamos contratado. Sin embargo, en este proyecto ya se contaba con una línea analógica dentro del laboratorio que permitía conectar nuestra centralita con la RTC. Por ello, ha sido necesario disponer de un dispositivo ATA, conversor analógico/digital, que transforme las señales VoIP de telefonía digital en señales analógicas de la telefonía convencional.

Para ello se ha utilizado un adaptador analógico modelo SPA3102 [32] de Linksys (Ilustración 83). Este elemento cuenta con varios puertos a los que debemos conectar nuestros dispositivos: línea telefónica, teléfono analógico, LAN Ethernet y WAN. Aunque no hemos utilizado todas sus características, es necesario destacar que también funciona en sentido inverso, pudiendo convertir señales VoIP para

comunicarse con teléfonos analógicos tradicionales. Además puede funcionar como conmutador siendo posible conectar directamente un teléfono IP o analógico y una línea ADSL o analógica y que funcione correctamente sin necesidad de una centralita externa. Bien es cierto, que deberían variarse los parámetros de configuración. Se ha utilizado para conectar la roseta de telefonía analógica por un extremo y el switch donde se encuentra nuestra red al otro.



Ilustración 83: Montaje de ATA conectado a router

Nuestra implementación necesita que la señal analógica que llega desde la RTC se convierta a señal VoIP que pueda ser recogida por la centralita Asterisk y viceversa. Se debe conectar el ATA (*Analog Telephony Adapter*) como intermediario entre el PTR y nuestra centralita. Usaremos el puerto de línea analógica para conectar con un RJ-45 al PRT y el puerto de Internet (que actúa como salida después de la conversión) al equipo switch de nuestra red local. El puerto Ethernet sería útil en el caso de poseer teléfonos IP y para la configuración inicial. La primera vez que accedemos al panel de configuración es necesario conectarse con el equipo mediante la interfaz LAN Ethernet debido a que la administración remota está desactivada por defecto. Una vez activado podemos acceder al panel de configuración mediante la interfaz de Internet sin problema.

### 6.2.1 Configuración del ATA SPA-3102

Se detallarán a continuación los pasos necesarios para configurar correctamente los parámetros del conversor analógico/digital para conseguir enviar y recibir llamadas desde y hacia cualquier teléfono conectado a la RTC. En la Ilustración 84 puede observarse el conexionado (puerto LINE hacia el PTR y puerto Internet hacia la red local).



Ilustración 84: Detalle de los puertos utilizados en el ATA

Al acceder al panel de control del ATA se debe cambiar la configuración de red por defecto para adecuarla al despliegue realizado. El interfaz web de configuración se puede observar en la Ilustración 85. Se mostrarán los aspectos clave de la configuración realizada para operar con nuestra implementación. Comenzaremos configurando la pestaña *WAN Setup* (Ilustración 86), en ella se introducen los parámetros necesarios para habilitar la comunicación IP dentro de la red (dirección local, dirección del Gateway y máscara de red).

**LINKSYS®**  
A Division of Cisco Systems, Inc. Linksys Phone Adapter Configuration

Router | Voice

Status | **Wan Setup** | Admin Login basic | advanced

**Product Information**

Product Name:	SPA-3102	Serial Number:	FM600G508087
Software Version:	5.1.7(GW)	Hardware Version:	1.4.5(a)
MAC Address:	000E08CD7662	Client Certificate:	Installed
Customization:	Open		

**System Status**

Current Time:	1/3/2003 12:34:54	Elapsed Time:	1 day and 22:40:33
Wan Connection Type:	DHCP	Current IP:	204.11.194.94
Host Name:	SipuraSPA	Domain:	callcentric.biz
Current Netmask:	255.255.255.192	Current Gateway:	204.11.194.65
Primary DNS:	66.193.176.41		
Secondary DNS:	204.11.193.12 204.11.192.20		
LAN IP Address:	192.168.0.1	Broadcast Pkts Sent:	3
Broadcast Bytes Sent:	1026	Broadcast Pkts Recv:	21434
Broadcast Bytes Recv:	2990023	Broadcast Pkts Dropped:	0
Broadcast Bytes Dropped:	0		

Undo All Changes | Submit All Changes

Admin Login basic | advanced

Ilustración 85: Panel de configuración SPA 3102

**Static IP Settings**

Static IP:	<input type="text" value="192.168.100.20"/>	NetMask:	<input type="text" value="255.255.255.0"/>
Gateway:	<input type="text" value="192.168.100.1"/>		

Ilustración 86: Configuración de red en el ATA

Como no se va a utilizar el dispositivo como router sino como convertidor de señales de voz, se configuran directamente los parámetros de la pestaña *Voice*. Luego, en la sección *PSTN Line* configuraremos la entrada de la RTC. Los campos a configurar son los mostrados en la Tabla 12.

Parámetro	Valor	Descripción
Line Enable	yes	Activación del puerto PSTN (RTC)
Proxy	192.168.100.50	Dirección IP del servidor Asterisk
User ID	psn	Nombre de usuario de la extensión SIP configurada en Asterisk
Password	*****	Contraseña de la extensión SIP configurada en Asterisk
Preferred Codec	G711u	Es posible escoger otros diferentes mientras sean soportados por la extensión de Asterisk
Dial Plan 1	(xx.)	Para llamadas salientes: significa que saldrán por la línea PSTN sin ninguna modificación de parámetros
Dial Plan 2	S0<: <a href="#">s@192.168.100.50</a> >	Para llamadas entrantes: las llamadas entrantes se dirigirán al Asterisk con la extensión s como destino
VoIP-To-PSTN Gateway Enable	yes	Permite el paso de llamadas VoIP hacia la RTC
PSTN Calles Auth Method	none	No se pedirá autenticación a las llamadas que provengan de la RTC
PSTN Ring Thru Line 1	no	No se conectará ningún teléfono analógico al ATA
PSTN Caller Default DP	2	Se utilizará el Dial Plan 2 para las llamadas entrantes
Disconnect Tone	425@-10; 10 (0.2/0.2/1,0.2/0.2/1,0.2/0.6/1)	Los tonos de desconexión varían según cada país, se ha configurado el tono válido para todo el Estado español

Tabla 12: Configuración de línea PSTN (RTC) en el SP3102

Aunque el ATA está configurado correctamente no podrá conectarse con Asterisk debido a que no se ha creado la extensión necesaria ni el enrutamiento dentro de la centralita. Dentro de la configuración de Asterisk se explicará el modo de comunicar ambos sistemas.

## 6.2.2 Configuración de la PBX Asterisk

Dentro de Asterisk las configuraciones a realizar son dos. Como se explicó en la sección de interconexión de OpenBSC con Asterisk, es preciso configurar extensiones SIP y su enrutamiento. En este caso el ATA o la conexión a la RTC será tratado por Asterisk como una extensión SIP y tendrá un tratamiento para las llamadas entrantes y salientes.

### 6.2.2.1 Extensión SIP equivalente al ATA

La configuración de la extensión que permite comunicarse con el SPA3012 es la siguiente:

```
[pstn]
type=friend
secret=pstn
qualify=yes
nat=no
insecure=very
host=dynamic
directmedia=no
context=from-pstn
dtmfmode=rfc2833
language=es
callerid=LineaTel
allowtransfer=yes
allowsubscribe=yes
subscribecontext=subscribe
callcounter=yes
disallow=all
allow=g711u
```

Los parámetros son muy similares a la extensión SIP configurada anteriormente aunque es necesario añadir algunas opciones diferentes. El contexto en este caso es *from-pstn* que se deberá configurar posteriormente en el archivo *extensions.conf*. Además se ha añadido *allow=g711u* para que acepte la codificación seleccionada para las llamadas en el ATA.

### 6.2.2.2 Nuevo contexto para llamadas entrantes y adición para llamada salientes

#### Llamadas entrantes:

Las llamadas que provengan desde la RTC pasarán a través del ATA y llegarán a Asterisk desde la extensión *pstn*. Debe crearse un contexto para manejar dichas llamadas. En un primer intento se ha configurado de la siguiente manera:

```
[from-pstn]
exten => s,1,Answer
exten => s,n,WaitExten(100)
exten => _XXXX,1,Goto(btsctrl,${EXTEN},1)
exten => _XXXX,n,Hangup
```

Las dos primeras entradas indican que las llamadas realizadas desde la extensión *pstn*, que estarán dirigidas a la extensión *s* tal y como se configuró en el ATA, será contestada y nos mantendremos a la espera 100 segundos para que se indique el número de extensión a marcar. Las dos siguientes enviarán la llamada según los números marcados hacia la extensión móvil de la BTS seleccionada. Se trata de una primera configuración se ha realizado a modo de prueba y no ha resultado funcional. El problema es que el ATA se encuentra conectado a una de las líneas de la centralita del GIT de la Universidad de Cantabria. Según la configuración anterior es necesario

introducir desde cualquier teléfono exterior el número de cabecera de la centralita, para luego marcar la extensión tras la que se encuentran los equipos.

En este punto se ha encontrado un problema debido a que la centralita del GIT cuando dirige la llamada hacia el contexto deseado, deja de mantenerse a la escucha de nuevas cifras que indique el abonado con el que se desea contactar. Por ello, para comprobar la funcionalidad del sistema se ha modificado la configuración de la siguiente forma:

```
[from-pstn]
exten => s,1,Answer
exten => s,n,Dial(LCR/GSM/2003,20)
exten => s,n,Hangup
```

Ahora, en lugar de esperar el marcado de la extensión directamente se dirige la llamada hacia una extensión (la 2003 del grupo LCR/GSM).

### Llamadas salientes:

Las llamadas salientes realizadas desde la red GSM no necesitan ser tratadas como un perfil nuevo sino que basta con actualizar el perfil existente *btsctrl* tal y como se observa a continuación:

```
exten => _9.,1,Answer
exten => _9.,n,Dial(SIP/pstn,45,D(${EXTEN:1}))
exten => _9.,n,Hangup
```

Con esta configuración, si se desea marcar un número externo es necesario primero marcar el 9 para que Asterisk sea consciente de que la llamada se dirige a un destino de la RTC. Además también se deberá marcar un 0 adicional para indicar a su vez a la centralita del GIT que se trata de un destino externo. Por tanto es necesario marcar el 90XXXXXXXXX donde las X's representan el número de abonado con el que se desea contactar. La conexión física de los elementos quedaría entonces como muestra la Ilustración 87.

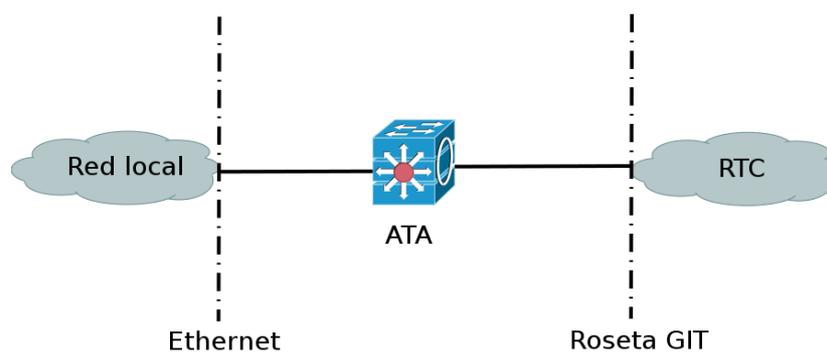


Ilustración 87: Esquema de conexión ATA

### 6.2.3 Uso y operación del sistema para comunicación con la RTC

Teniendo todos los elementos configurados y conectados adecuadamente se procede a evaluar el funcionamiento del sistema. En este caso se debe notificar a *osmo-nitb* que se ha conectado a la RTC para lo que se añade la opción -P.

Las pruebas realizadas para las llamadas entrantes y salientes han resultado satisfactorias. Por una parte, llamando desde la extensión móvil de OpenBSC a un teléfono móvil operando en una red de otro operador. Se realiza como una llamada normal pero anteponiendo el prefijo 90 antes del número de teléfono al que se desea llamar.

Para comprobar el servicio en el sentido contrario, se utiliza un teléfono móvil conectado a la red de un operador común y se marca en primer lugar el número de cabecera de la centralita del GIT. Una locución nos indica que se debe introducir el número de extensión dentro del departamento GIT de la Universidad de Cantabria anteponiendo el 0. Marcamos 0510 ya que la extensión asignada a la roseta que hemos utilizado es el 510. Tras unos segundos observamos que la extensión 2003 indica que tiene una llamada entrante.

### 6.3 Opciones y ventajas del proyecto OpenBSC

En el presente capítulo se ha mostrado cómo se puede realizar, de forma sencilla mediante el proyecto OpenBSC, una implementación bastante completa de una celda GSM perfectamente operativa. Esto abre un gran campo de estudio ya que el estándar GSM es implantado únicamente por operadores cerrados y no es posible en la mayoría de los casos realizar pruebas en una red transparente. Por ello el enorme potencial del presente proyecto es proporcionar un entorno de pruebas para conocer el entramado de los protocolos y las directivas del estándar GSM pudiendo incluso configurar y variar parámetros de antenas y elementos GSM para estudiar la variación en el rendimiento de la red. La idea principal es conocer los aspectos de GSM que de otra forma podrían ser únicamente estudiados mediante libros y estándares de comunicaciones. Con una celda GSM propietaria, tenemos el control de todas las partes de la comunicación y podemos realizar diversas pruebas hasta conseguir la configuración deseada en cada uno de los elementos que componen la red. Se evita de este modo la necesidad de solicitar permisos a los operadores de telefonía.

Ítem	Marca	Modelo	Función	Precio
Teléfonos móviles GSM	Cualquiera	Cualquiera	Realizar llamadas y comprobar el funcionamiento de la celda	Desde 30€
nanoBTS	ip.access	1800/0/0	Hardware que implementa la parte radio de la estación base	4000 €
PC	Cualquiera	Cualquiera	Ejecutar los programas utilizados para controlar la nanoBTS y la PBX	Desde 200€
Convertor digital/analógico	Linksys	SPA3102	Conectar protocolo VoIP con la telefonía analógica tradicional	42 €

Tabla 13: Modelos y precio de los componentes del sistema

Otra gran ventaja de este desarrollo no es la propia red comunicaciones, sino que una vez que tenemos nuestra celda operativa podemos realizar pruebas de comunicación entre dispositivos compatibles sin necesidad de contratar los servicios de los operadores comerciales y realizar un desembolso para cubrir las tarifas que nos ofrecen. Un buen ejemplo podría ser un entorno de pruebas de alguna empresa que utilice equipos GSM para la transmisión de comunicaciones de voz. Podría, mediante

la utilización de esta red, testear los equipos sin necesidad de acogerse a las tarifas de los operadores y creando un escenario a su medida.

Estamos hablando de un entorno de válido para ofrecer cobertura en entornos de poca capacidad como pueden países en desarrollo o un barco en alta mar en el que los tripulantes pudiesen utilizar su terminal GSM para realizar llamadas a través de una centralita conectada a un enlace vía satélite. La cobertura se ha limitado con el fin de no interferir con los terminales de operadores situados fuera del laboratorio pero en un entorno libre podría dar servicio a terminales situados a varios cientos de metros de la estación base.

Se ha de tener en cuenta que el material utilizado para la realización del proyecto es fácilmente accesible y su coste es muy reducido en comparación con el equipamiento utilizado por los operadores de telefonía móvil. Cabe destacar también que la fiabilidad y el número de usuarios en éste caso dista mucho de las implementaciones comerciales pero sigue siendo un perfecto campo de pruebas en entornos reducidos. En la Tabla 13. se muestran los detalles de los elemento utilizados y esto pueden verse en la Ilustración 88.



**Ilustración 88: Equipos utilizados para OpenBSC + Asterisk + ATA**

Todos los elementos tienen un coste asumible cuando se trata de realizar un entorno bien educativo o bien empresarial para obtener una red GSM totalmente abierta donde pueden realizarse todo tipo de configuraciones y pruebas libremente. Hay que tener en cuenta las limitaciones legales debido a que estas pruebas deben ser realizadas dentro de laboratorios cerrados sin que las emisiones radio interfieran con las frecuencias asignadas a las operadoras.

Por último indicar, que podría servir como solución de compromiso dentro de zonas con escasa demanda de clientes en las que la inversión por parte de los operadores

de telefonía no es viable y en muchas ocasiones es subvencionada por el estado. Aunque el funcionamiento podría verse alterado ya que no es una implementación madura y no ha sido probada en grandes entornos, puede ser interesante para optimizar recursos y llevar cobertura GSM a zonas que han sido descartadas. El problema al que podemos enfrentarnos en entornos extensos es la cobertura, pero además de que puede aumentarse la potencia de emisión de la BTS, existen amplificadores de señal que no elevarían demasiado el coste total.

## 6.4 Seguridad del estándar GSM

A pesar de que el estándar GSM es actualmente el más utilizado dentro de las redes de comunicaciones móviles, cuenta con algunos agujeros de seguridad importantes. Además, debido a la aparición de las nuevas generaciones de telefonía móvil, los vectores de ataque no se han intentado frenar ya que los estándares siguientes ya hacían frente a los mismos. Se mostrará un ejemplo de ataque práctico aprovechando uno de los agujeros de seguridad de GSM.

### 6.4.1 Falta de autenticación mutua

Las redes de comunicaciones, al menos las modernas y sobre todo las que utilizan el interfaz radio, están dotadas de mecanismos que permiten que los extremos de la comunicación conozcan a nivel enlace la identidad de su par. Unos de los problemas que existen en el estándar GSM es que la red si necesita que el móvil se identifique y que se produzca un intercambio de claves para verificar que el abonado es quien dice ser, pero no es así en el sentido contrario. El estándar no contempla y por lo tanto, los fabricantes no implementan ningún mecanismo que asegure al terminal móvil que la estación base pertenece al operador con el que tiene un contrato vigente.

En ningún momento durante el proyecto se ha indicado la autenticación del terminal móvil siguiendo los protocolos del estándar. Se debe a que debido a otro agujero de seguridad, podemos operar con los terminales sin que se produzca la autenticación. El truco es que el software que controla la BTS indica al móvil que este debe operar sin claves y el terminal actúa de la forma en la que le indica la estación, haciendo innecesaria la implementación del mecanismo de autenticación. De esta manera se puede realizar el “ataque mediante estación base falsa [33]”.

### 6.4.2 Ataque a las comunicaciones de voz GSM mediante estación base falsa

En el presente proyecto se dispone de una infraestructura de red GSM completa y a la que los terminales pueden acceder como si se tratase de una red comercial convencional. Bastará pues configurar los parámetros de la red radiada por nuestra antena con los mismo códigos que la red de un operador estándar y conseguir que la cobertura proporcionada por ella sea mayor que la ofrecida por las antenas del operador más próximas, para que el terminal se conecte a nuestra implementación en lugar de a la red convencional. Los códigos MCC, que indican el país en que se aloja la red, y el MNC, identificador de la red del operador, deben ser idénticos.

A partir de aquí, es relativamente sencillo gracias al PC Linux que alberga el controlador de las estaciones base, realizar ataques a los terminales para obtener información de sus comunicaciones. Se expondrán a continuación el ejemplo de un ataque a para las comunicaciones de voz. En ambos caso se parte del escenario en el que tenemos los sistemas mostrados en apartados anteriores funcionando correctamente y el terminal objetivo campeando dentro de nuestra red ignorando que no es realmente la red de su operador.

Gracias la PBX Asterisk instalada en el *host* que controla la estación base, podemos redirigir las llamadas que éste realice a cualquier destino que deseemos. Esto tiene unas implicaciones muy graves debido a que algunas de esas llamadas pueden tener destinos tan comprometidos como bancos u otros servicios donde pueda ser necesario solicitar al cliente claves y datos personales.

Imaginemos por ejemplo, que creamos un enrutamiento en Asterisk por el cual el número de servicio del banco del abonado se dirige hacia nuestro número de teléfono. Podría pensarse que en la mayoría de los caso aparece una locución del banco que nos indica las opciones y por ello no podríamos suplantar al banco pero, también gracias a Asterisk es posible almacenar dicha locución dentro del fichero de sonidos y en el mismo archivo de enrutamiento incluir una locución antes de que la llamada llegue a su destino. Como se muestra a continuación, debemos tras la locución debemos dirigir la llamada al ATA para que marque un número externo.

```
[externas]
exten => 902XXXXXX,1,Answer()
exten => 902XXXXXX,2,Playback(locucion)
exten => 902XXXXXX,3,Dial(SIP/spa3102,45,942XXXXXX)
exten => 902XXXXXX,4,Hangup()
```

Al recibir la llamada no tendremos más que solicitar al cliente los datos necesarios para poder suplantar su identidad, como podrían ser las claves de acceso a sus cuentas. Es por esto que los banco y otros entidades similares, no solicitan las claves ni datos personales que puedan comprometer la seguridad. En caso de necesitar contraseñas solicitan sólo algunos dígitos de las mismas para que ataques de éste tipo no puedan completarse con éxito. La forma de combatir éstos ataques es mediante la protección del espectro licenciado no permitiendo emitir en las bandas de frecuencia en las que opera el estándar teniendo que abonar en caso de infracción cuantiosas multas.

### 6.4.3 Extensión del ataque a otras redes de comunicaciones

El ataque mostrado anteriormente no es cálido para los siguientes estándares de comunicaciones móviles (UMTS y LTE). Esto es debido a que si que existe una autenticación mutua dentro de la red por lo que la estación base también debe demostrar al terminal que realmente pertenece al operador.

Junto con el problema anterior, tenemos que terminales de telefonía actuales cuentan con capacidad para conectarse a redes de tecnologías móviles de tercera e incluso de cuarta generación. Además por defecto, se conectarán siempre a la red más rápida disponible por lo que el ataque anterior resulta más complicado de realizar. La única opción es anular la cobertura de las redes 3G y 4G para obligar al terminal a utilizar la red GSM.

## Capítulo 7 – Conclusiones y líneas futuras

## 7 Conclusiones y líneas futuras

Una vez finalizado el proyecto es el momento de hacer el análisis de los que se ha realizado, lecciones aprendidas y ver las líneas futuras de lo que se podrá hacer partiendo de esta base. En ese sentido se analizarán las dos partes que lo componen por separado. Por un lado la del analizador y la de la red. Aunque ambas pueden estar internamente relacionadas pues la red implementada se podría analizar con la herramienta de análisis propuesta.

Como punto común de ambos bloques se tiene que se ha conseguido realizar la misma funcionalidad que equipos comerciales muy superiores en precio. Bien es cierto que el alcance de los mismos se restringe a un entorno de laboratorio con unas exigencias menos restrictivas pero se ha visto que cumplen su función de forma satisfactoria. A continuación se describen los aspectos más importantes que se han observado mediante la realización del presente proyecto.

### 7.1 Analizador de redes GSM

Se pasarán a describir las implicaciones de la implementación del equipo de análisis de un estándar de comunicaciones móviles GSM. Aunque las capacidades de las configuración actual han resultado suficientes para un estudio general, la parte software de la implementación tiene un gran desarrollo futuro que puede convertirlo en una herramienta muy potente para la educación y para las empresas.

#### 7.1.1 Implicaciones del analizador de redes

Con un presupuesto muy ajustado se ha conseguido realizar un analizador de redes bajo el estándar GSM con las siguientes funcionalidades:

- Captura de tráfico GSM en tiempo real
- Observación de medidas de potencia y ocupación de los canales
- Análisis de tramas GSM

Estas herramientas nos permiten de una forma sencilla, el estudio de las redes de comunicaciones móviles de segunda generación. Podemos obtener gran cantidad de información sobre el funcionamiento de los procedimientos de llamada, acceso a la red, envío de SMS... Desde el punto de vista académico resulta una excelente manera de mostrar el funcionamiento de las redes desde dentro con entornos de captación de datos reales sin necesidad de simuladores. Este apartado es quizás uno de los más importantes puesto que GSM se trata de una tecnología de muy amplio acceso como usuario pero un acceso tremendamente restringido como gestor. La infraestructura pertenece a operadores comerciales que no facilitan documentación ni acceso a la misma haciendo muy difícil su estudio en organismos educativo no vinculados a estas empresas.

No menos importante es el punto de vista comercial. Mediante la utilización de este sistema se pueden realizar muchas medidas de potencia de recepción de señal, número de operadores en una zona, calidad de las señales radio... Esto puede ser muy interesante desde el punto de vista económico para elegir la ubicación de equipos que dispongan de conectividad GSM o para la elaboración de estadísticas como la

contaminación electromagnética. Además puede utilizarse para evaluar la carga de las redes en cuanto a tráfico y congestión una vez implementadas y prever posibles ampliaciones. Se trata de una solución muy simple y con un coste muy bajo y podría ser una opción muy a tener en cuenta cuando no existen unos requisitos demasiado estrictos.

Se han citado ejemplos en los que la implementación realizada podría ser muy válida y constituiría una opción a tener en cuenta para recoger datos, procesos e información sobre el estándar GSM. Pero aún queda camino por recorrer y existe una potente comunidad de desarrolladores dentro de OsmocomBB que continúan ampliando las capacidades del analizador.

### 7.1.2 Líneas futuras del analizador de redes

Aunque en el presente proyecto no se ha participado en las nuevas implementaciones que se están llevando a cabo dentro del proyecto OsmocomBB, durante el análisis y las pruebas realizadas con las características ya existentes, se ha mantenido contacto con la comunidad de desarrolladores.

Actualmente los objetivos principales son trasladar el los niveles 2 y 3 de GSM al propio terminal móvil. De esta manera se pretende liberar del trabajo de procesamiento a los PC's y así lograr terminales de bajo coste capaces de funcionar como analizadores de tramas de forma aislada. Además se está trabajando también para la generación de reportes de medidas y que éstas sean fácilmente exportables a formatos con lo que poder trabajar y manejar los datos de forma sencilla.

Por último, durante el tiempo que se ha trabajado con el material propuesto por el proyecto, se ha observado que la comunidad de desarrolladores se encuentra trabajando para añadir nuevos terminales a lista de compatibles. Por un lado, se buscan terminales de bajo coste pero que los fabricantes sigan ofreciendo en su catálogo para que sea sencillo y asequible hacerse con ellos. Por otra parte, se está investigando con terminales de última generación que al estar dotados de mayor capacidad de procesamiento y un sistema operativo dentro del cuál es más sencillo realizar programas, podrían ser una herramienta mucho más manejable a la hora de implementar nuevas características.

Debido a que el código del software es completamente abierto y accesible a cualquiera que esté interesado por el proyecto OsmocomBB, las posibilidades de ampliación son muy grandes. Como inicio cabe destacar que las interfaces están muy poco desarrolladas debido a que se trata de algo experimental. Esto implica que un punto muy interesante sería implementar interfaces que permitiesen mostrar los datos de forma más amigable, realizar gráficos, manejo mediante ventanas con botones... De esta manera se crearía un software que podría realizar mapas de cobertura, historiales de evolución de calidad de señal o evaluación en el tiempo de la carga dentro de una celda. Las posibilidades que esto ofrece a la hora de gestionar redes en tiempo real, modificación de parámetros según el estado de la red o simplemente el estudio y conocimiento de un estándar de comunicaciones móviles ampliamente extendido son enormes.

Por el contrario hablamos de un software libre sin interés comercial y que las compañías telefónicas, quienes realmente hacen un uso intensivo, cuentan con software privado potente que realiza el análisis y mantenimiento de las redes de forma muy eficiente. No obstante, como podría ser útil en situaciones de baja exigencia

como núcleos pequeños de población o para tareas no demasiado restrictivas en cuanto al margen de error de los datos.

## 7.2 Estación base GSM

La segunda parte del presente proyecto tiene una serie de implicaciones semejantes a las del apartado anterior desde el punto de vista académico y comercial. Pero a su vez cuenta con valor añadido que podría resultar de mucha utilidad a la hora de implementar sistemas GSM comerciales en entornos poco exigentes como pequeños núcleos de población, refuerzo de los sistemas existentes en eventos donde es necesario ampliar la capacidad para una afluencia de usuarios mayor a la dimensionada o países en vías de desarrollo.

### 7.2.1 Implicaciones de la estación base

En primer lugar, conseguir un sistema GSM de bajo coste, funcional y capaz de comunicarse con otras redes de telefonía y datos de diversa naturaleza es de vital importancia desde el punto de vista académico para conocer el funcionamiento de la segunda generación del estándar de comunicaciones móviles. Gracias a las opciones que ofrece el montaje, se pueden comprobar gran cantidad de parámetros inherentes a las redes móviles y variar su configuración para estudiar los efectos que éstos producen sobre la red y las comunicaciones. Serviría entonces como entorno de pruebas para el estudio y comprobación sobre el terreno y en un entorno cercano a la realidad, del funcionamiento de GSM.

Pero además también resultaría de vital importancia para empresas que hagan uso de esta tecnología como medio de transmisión de información entre sus equipos. Actualmente los operadores imponen fuertes restricciones a la hora de realizar pruebas sobre su infraestructura y tarifican además el tráfico consumido por los usuarios. Con una pequeña inversión podrá obtenerse una implementación de red que soporta gran parte de los servicios pero libre de todo coste recurrente por el tráfico y de cualquier restricción en cuanto a configuración de los equipos.

Otra opción ofrecida por este proyecto y que ha de tenerse en cuenta, es que al poseer los servicios básicos que requieren los usuarios dentro de las redes GSM, podría ser una alternativa viable para los operadores de telefonía convencionales. Los escenarios donde podría resultar interesante la instalación ya sea permanente o circunstancial de estas implementaciones son muy dispares:

- Pequeños núcleos de población con baja densidad de clientes
- Eventos donde se concentra un mayor volumen de clientes que el dimensionado por la red que dota de cobertura a la zona
- Países en desarrollo donde el número de abonados es demasiado bajo

El interés en instalar este tipo de soluciones para los casos anteriores es un principalmente el ahorro por parte de los proveedores en infraestructura y en consumo energético. En algunos de los escenarios propuestos el suministro eléctrico es difícilmente accesible y es necesario el uso de generadores que conllevan un fuerte gasto para las compañías. En otros simplemente, no resultaría rentable instalar un sistema GSM convencional para dar servicio a un número potencial de clientes demasiado bajo. La gran ventaja en cualquier caso es la gran extensión de las redes

de segunda generación y por tanto el elevado número de terminales disponibles en el mercado compatibles con la misma.

Además, el proyecto OpenBSC continúa aún en desarrollo tratando de conseguir redes más estables, una mejor interconexión entre sus propios elementos y con otras redes e intentando parecerse cada día más al funcionamiento intrínseco de las redes GSM. A continuación se muestran los objetivos de ambos proyectos para el futuro.

### 7.2.2 Próximos objetivos del proyecto OpenBSC

Aunque el proyecto está muy avanzado y la plataforma OpenBSC soporta servicio de mensajería y voz complemente además de ofrecer soluciones para integrarse con otras redes de comunicaciones, cuenta con una gran comunidad de desarrolladores que revisan cada día el código para mejorarlo y tratan de implementar nuevos servicios. Dentro de los servicios ya existentes se buscan mejorar características y evitar los errores, que aunque son muy pocos, ocurren en algunas partes de los programas. Se intenta también hacer más amigable la instalación y la configuración del software y el hardware con el fin de abrir la comunidad y conseguir que un mayor número de personas se interese por el proyecto y contribuya a mejorarlo.

Dentro de los objetivos de implementación de nuevos servicios se está trabajando en características como los mensajes de *broadcast* dentro de la celda, el cifrado de las comunicaciones, las llamadas de emergencia... En definitiva el objetivo es conseguir toda la operatividad del estándar GSM y las opciones que ofrece intentando respetar los protocolos y las directivas de funcionamiento que marca la especificación del estándar. De todos modos, como se ha podido comprobar, el estado del proyecto es muy avanzado y con las características disponibles se puede llegar a conseguir una celda GSM perfectamente funcional y operativa.

### 7.2.3 Proyecto OpenBSC\_GPRS

A día de hoy se encuentra también en desarrollo un proyecto paralelo a OpenBSC llamado OpenBSC\_GPRS [34] que busca añadir a la red actual el estándar GPRS para la transmisión de datos sobre redes GSM.

El planteamiento consiste, de forma similar a lo que ocurre en las redes comerciales, de implementar los componentes de GPRS sobre los ya existentes. Además, debido a la naturaleza IP de los datos y la extensión de este tipo de redes, resulta más sencilla la conexión de nuestra estación base con la red Internet. Se realiza mediante el propio sistema operativo creando nuevos interfaces de redes que redirigen el tráfico generado y entrante hacia fuera de la red y en sentido inverso.

El proyecto se encuentra en fase de desarrollo por lo que existen problemas a la hora de su instalación resultado poco estable en muchas ocasiones pero el equipo de desarrolladores está trabajando de forma intensa para que pueda llegar a ser tan útil como la parte de GSM.

## Capítulo 8 – Bibliografía

## 8 Bibliografía

- [1] Biografía de Guillermo Marconi – Biografías y Vidas  
<http://www.biografiasyvidas.com/biografia/m/marconi.htm>
- [2] Ya hay 6.000 millones de línea móviles en el mundo, según una agencia de la ONU – Tecnología: ABC.es  
<http://www.abc.es/20121015/tecnologia/abci-numero-moviles-mundo-201210151531.html>
- [3] Apple intenta competir con los ISP tradicionales – ADSL Zone  
<http://www.adslzone.net/article4956-las-grandes-companias-se-aponen-a-que-apple-se-convierta-en-operador-movil-virtual.html>
- [4] Comunicaciones móviles  
Mónica Gorriacho Moreno y Juan Luis Gorriacho Moreno – Ediciones UPC, Febrero 2002
- [5] RECOMENDACIÓN UIT-R M.1036-2  
Disposiciones de frecuencias para la implementación de la componente terrenal de las telecomunicaciones móviles internacionales-2000 (IMT-2000) en las bandas\* 806-960 MHz\*\*, 1710-2025 MHz, 2110-2200 MHz y 2500-2690 MHz
- [6] Mobile Telecommunications: Standards, Regulation, and Applications  
Rudi Bekkers (Artech House Mobile Communications Library)
- [7] LTE Smart Analyzer - RADCOM  
[http://www.radcom.com/LTE\\_Smart\\_Analyzer](http://www.radcom.com/LTE_Smart_Analyzer)
- [8] Analizador GSM K15 Tektronix – Livingstone Rental  
[http://www.livingstonrental.es/p\\_tektronix/telecomunicaciones-radiocomunicaciones/comprobadores-de-estaciones-base-y-terminales/tektronix-k15/](http://www.livingstonrental.es/p_tektronix/telecomunicaciones-radiocomunicaciones/comprobadores-de-estaciones-base-y-terminales/tektronix-k15/)
- [9] Cuadro nacional de atribución de frecuencias (CNAF)  
Ministerio de Industria, Energía y Turismo  
<http://www.minetur.gob.es/telecomunicaciones/Espectro/Paginas/CNAF.aspx>
- [10] La subasta del espectro de telefonía móvil se cierra con un precio final de 1.647 millones – EuropaPress  
<http://www.europapress.es/portaltic/sector/noticia-subasta-espectro-telefonía-movil-cierra-precio-final-1647-millones-20110729185123.html>
- [11] Operadoras móviles virtuales en España – Operadoras móviles  
<http://operadoras-moviles.com/omvs/>
- [12] Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones  
«BOE» núm. 264, de 4 de noviembre de 2003
- [13] LTE – 3GPP  
<http://www.3gpp.org/LTE>
- [14] ONO Wifi  
<https://www.onowifi.es/es/>

[15] Proyecto OsmocomBB – Osmocom  
<http://bb.osmocom.org/trac/>

[16] WireShark – Wireshark Foundation  
<http://www.wireshark.org>

[17] GSMTAP – OsmocomBB  
<http://bb.osmocom.org/trac/wiki/GSMTAP>

[18] Home – Smart Card Alliance  
<http://www.smartcardalliance.org>

[19] GSM 11.11 ETSI TS/SMG-091111QR1  
Specification of the Subscriber Identity Module – Mobile Equipment (SIM - ME)  
interface. Versión 5.3.0. July 1996.

[20] GSM 03.40 ETSI TS/SMG-040340QR2  
Technical realization of the Short Message Service (SMS) – Point-to-Point (PP)  
Versión 5.3.0. July 1996.

[21] Un 'hacker' descifra el código de cifrado del sistema GSM – El Mundo  
<http://www.elmundo.es/elmundo/2009/12/29/navegante/1262094278.html>

[22] Software para acceder a GPRS desde un Motorola C123 – El informático  
<http://elinformatico.eu/crean-un-software-para-acceder-a-datos-gprs-desde-un-motorola-c-123-20110811>

[23] Proyecto OpenBSC – Osmocom  
<http://openbsc.osmocom.org/trac/>

[24] What is OpenBTS? – OpenBTS  
<http://openbts.org>

[25] Enterprise and Public Access: Small cells for complex coverage – ip|access  
<http://www.ipaccess.com/en/public-access>

[26] RFC 2131 – Dynamic Host Configuration Protocol  
R. Droms – Bucknell University. March 1997

[27] Asterisk  
<http://www.asterisk.org>

[28] Linux-Call-Router  
<http://isdn.eversberg.eu>

[29] Telephone Mac App - Alexei Kuznetsov  
<http://www.tlphn.com>

[30] MegaVoip – Mega cheap, mega good quality  
<http://www.megavoip.com/rates/>

[31] EasyVoip – The cheapest international calls  
<http://www.easyvoip.com/dashboard>

[32] SPA3102 Voice – Linksys (Cisco)

<http://www.cisco.com/en/US/products/ps10027/index.html>

[33] Un ataque práctico contra comunicaciones móviles – RootedCon Marzo 2011

David Perez y Jose Pico

[34] OpenBSC\_GRPS - Osmocom

[http://openbsc.osmocom.org/trac/wiki/OpenBSC\\_GPRS](http://openbsc.osmocom.org/trac/wiki/OpenBSC_GPRS)

## Capítulo 9 – Acrónimos

## 9 Acrónimos

### A

**AMPS:** Advanced Mobile Phone System  
**API:** Application Programming Interface  
**ARFCN:** Absolute Radio-Frequency Channel Number  
**ARM:** Acorn RISC Machine  
**ATA:** Advanced Technology Attachment

### B

**BCCH:** BroadCast Control Channel  
**BER:** Bit Error Rate  
**BSC:** Base Station Controller  
**BSIC:** Base Station Identify Code  
**BSS:** Base Station System  
**BTS:** Base Transceiver Station

### C

**CCCH:** Common Control Channels  
**CPU:** Central Processing Unit

### D

**DCS:** Digital Cellular Service  
**DHCP:** Dynamic Host Configuration Protocol  
**DSP:** Digital Signal Processor

### F

**FACCH:** Fast Associated Control Channel  
**FCCH:** Frequency Correction Channel

### G

**GGSN:** Gateway GPRS Support Node  
**GIT:** Grupo de Ingeniería Telemática  
**GMSC:** Gateway Mobile Switching Center  
**GPRS:** General Packet Radio Service  
**GSM:** Groupe Spécial Mobile

### H

**HLR:** Home Location Register

**I**

**ICCID:** Integrated Circuit Card ID  
**IMSI:** International Mobile Subscriber Identity  
**IP:** Internet Protocol  
**ISDN:** Integrated Services for Digital Network  
**ISP:** Internet Service Provider  
**ITU:** International Telecommunication Union

**J**

**JTAC:** Japanese Total Access Communication

**K**

**Ki:** Authentication Key

**L**

**LAC:** Location Area Code  
**LAN:** Local Area Network  
**LAPD:** Link Access Protocol for D-channel  
**LCR:** Linux Call Router  
**LGT:** Ley General de Telecomunicaciones  
**LTE:** Long Term Evolution

**M**

**MAC:** Media Access Control  
**MCC:** Mobile Country Code  
**MHz:** Mega Hercios  
**MNC:** Mobile Network Code  
**MNCC:** Mobile Network Call Control  
**MS:** Mobile Station  
**MSC:** Mobile Switching Center

**N**

**NMC:** Network Management Center  
**NSS:** Network and Switching System  
**NVRAM:** Non-Volatile Random-Access Memory

**O**

**OMC:** Operation and Management Center  
**OMV:** Operadora Móvil Virtual  
**OSS:** Operation Support System

**P**

**PAGCH:** Paging and Access Granted Channel  
**PBX:** Private Branch Exchange  
**PC:** Personal Computer  
**PDP:** Packet Data Protocol  
**PDU:** Packet Data Unit  
**PIN:** Personal Identification Number  
**PoE:** Power over Ethernet  
**PSTN:** Public Switched Telephone Network  
**PTR:** Punto de Terminación de Red

**R**

**RACH:** Random Access Channel  
**RAM:** Random-Access Memory  
**RDSI:** Red Digital de Servicios Integrados  
**RISC:** Reduced Instruction Set Computing  
**RLA:** Received Level Average  
**RR:** Request Reference  
**RTC:** Red Telefónica Conmutada  
**RTC:** Real Time Protocol

**S**

**SACCH:** Slow Associated Control Channel  
**SCH:** Synchronization Channel  
**SDCCH:** Standalone Dedicated Control Channel  
**SGSN:** Serving GPRS Support Node  
**SIM:** Subscriber Identity Module  
**SIP:** Session Initiation Protocol  
**SMS:** Short Message Service  
**SS7:** Signalling System 7

**T**

**TACS:** Total Acces  
**TCH/F:** Traffic Channel Full Rate  
**TCH/H:** Traffic Channel Half Rates Communication System  
**TCP:** Transmission Control Protocol  
**TRAU:** Transcoder / Rate Adapter Unit  
**TSMI:** Temporary Mobile Subscriber Identity

**U**

**UART:** Universal Asynchronous Receiver/Transmitter  
**UDP:** User Datagram Protocol  
**UMTS:** Universal Mobile Telecommunication System  
**USB:** Universal Serial Bus

## **V**

**VLR:** Visitor Location Register

**VoIP:** Voice over IP

## **W**

**WAN:** Wide Area Network

**WiFi:** Wireless Fidelity

## **3**

**3GPP:** 3rd Generation Partnership Project

## Capítulo 10 – Apéndices

## 10 Apéndices

### [Apéndice1] openbsc.cfg

```
!  
! OpenBSC (0.11.0.1-c513) configuration saved from vty  
!!  
password foo  
!  
log stderr  
  logging color 1  
  logging timestamp 0  
  logging level all everything  
  logging level rll notice  
  logging level cc notice  
  logging level mm notice  
  logging level rr notice  
  logging level rsl notice  
  logging level nm info  
  logging level mncc notice  
  logging level sms notice  
  logging level pag notice  
  logging level meas notice  
  logging level sccp notice  
  logging level msc notice  
  logging level mgcp notice  
  logging level ho notice  
  logging level db notice  
  logging level ref notice  
  logging level gprs debug  
  logging level ns info  
  logging level bssgp debug  
  logging level llc debug  
  logging level sndcp debug  
  logging level nat notice  
  logging level ctrl notice  
  logging level lglobal notice  
  logging level llapd notice  
  logging level linp notice  
  logging level lmux notice  
  logging level lmi notice  
  logging level lmib notice  
  logging level lsms notice  
!  
line vty  
  no login  
!  
e1_input  
  e1_line 0 driver ipa  
  e1_line 0 port 0  
network  
  network country code 214  
  mobile network code 29  
  short name OpenBSC
```

```
long name OpenBSC
auth policy closed
location updating reject cause 13
encryption a5 0
neci 1
paging any use tch 0
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
timer t3101 10
timer t3103 0
timer t3105 0
timer t3107 0
timer t3109 0
timer t3111 0
timer t3113 60
timer t3115 0
timer t3117 0
timer t3119 0
timer t3122 0
timer t3141 0
dtx-used 0
subscriber-keep-in-ram 0
bts 0
  type nanobts
  band DCS1800
  cell_identity 425
  location_area_code 8001
  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 1800 0
  oml ip.access stream_id 255 line 0
  neighbor-list mode automatic
  gprs mode egprs
  gprs routing area 0
  gprs cell bvci 2
  gprs cell timer blocking-timer 3
  gprs cell timer blocking-retries 3
  gprs cell timer unblocking-retries 3
  gprs cell timer reset-timer 3
  gprs cell timer reset-retries 3
  gprs cell timer suspend-timer 10
  gprs cell timer suspend-retries 3
  gprs cell timer resume-timer 10
```

```
gprs cell timer resume-retries 3
gprs cell timer capability-update-timer 10
gprs cell timer capability-update-retries 3
gprs nsei 101
gprs ns timer tns-block 3
gprs ns timer tns-block-retries 3
gprs ns timer tns-reset 3
gprs ns timer tns-reset-retries 3
gprs ns timer tns-test 30
gprs ns timer tns-alive 3
gprs ns timer tns-alive-retries 10
gprs nsvc 0 nsvci 102
gprs nsvc 0 local udp port 23000
gprs nsvc 0 remote udp port 23333
gprs nsvc 0 remote ip 192.168.100.50
trx 0
  rf_locked 0
  arfcn 770
  nominal power 23
  max_power_red 20
  rsl e1 tei 0
  timeslot 0
    phys_chan_config CCCH+SDCCH4
    hopping enabled 0
  timeslot 1
    phys_chan_config SDCCH8
    hopping enabled 0
  timeslot 2
    phys_chan_config TCH/F
    hopping enabled 0
  timeslot 3
    phys_chan_config TCH/F
    hopping enabled 0
  timeslot 4
    phys_chan_config TCH/F
    hopping enabled 0
  timeslot 5
    phys_chan_config TCH/F
    hopping enabled 0
  timeslot 6
    phys_chan_config TCH/F
    hopping enabled 0
  timeslot 7
    phys_chan_config PDCH
    hopping enabled 0
mncc-int
  default-codec tch-f efr
  default-codec tch-h hr
```

## [Apéndice2] sip.conf

```
[1001]
type=friend
context=btsctrl
host=dynamic
secret=1001
nat=no

[1002]
type=friend
context=btsctrl
host=dynamic
secret=1002
nat=no

[pstn]
type=friend
secret=pstn
qualify=yes
nat=no
insecure=very
host=dynamic
directmedia=no
context=from-pstn
dtmfmode=rfc2833
language=es
callerid=LineaTel
allowtransfer=yes
allowsubscribe=yes
subscribecontext=subscribe
callcounter=yes
disallow=all
allow=ulaw
allow=g729
```

## [Apéndice3] extensions.conf

```
; extensions.conf - the Asterisk dial plan
;
[general]
;
;
; Exclusive context for calls to PSTN
;
[from-pstn]
exten => s,1,Answer
exten => s,n,Dial(LCR/GSM/2004,20)
exten => s,n,Hangup
;exten => s,n,WaitExten(100)
;exten => _XXXX,1,Goto(btsctrl,${EXTEN},1)
;exten => _XXXX,n,Hangup
;
; Exclusive context for OpenBSC/LCR
;
[btsctrl]
include => externas

exten => _20XX,1,Answer
exten => _20XX,n,Dial(LCR/GSM/${EXTEN},20)
exten => _20XX,n,Hangup

exten => _10XX,1,Answer
exten => _10XX,n,Dial(SIP/${EXTEN},20)
exten => _10XX,n,Hangup

exten => _9.,1,Dial(SIP/pstn,45,D(${EXTEN:1}))
exten => _9.,n,Busy(3)
exten => _9.,n,Hangup
;
; Prueba para externas
;
[externas]
exten => 5555,1,Answer
exten => 5555,n,WaitExten(10)

exten => _XXXX,1,Goto(btsctrl,${EXTEN},1)
exten => _XXXX,n,Hangup
;
```

## [Apéndice4] routing.conf

```
# Linux-Call-Router routing configuration "routing.conf"

# Ruleset: MAIN
# Calls with different origins will be processed in different
# rulesets.

[main]
interface=GSM                : remote application=asterisk
context=btsctrl
extern                       : goto ruleset=extern
intern                       : goto ruleset=intern
                           : disconnect cause=31

# Ruleset: EXTERN
# All calls from external lines are processed here.

[extern]
dialing=1234 remote=asterisk : remote application=asterisk
dialing=0,1234              : intern extension=200
dialing=200-299             : intern
dialing=81                  : partyline room=42
#timeout=6                  : intern extension=200
default                     : disconnect cause=1
```

## [Apéndice5] interface.conf

```
# interface.conf
#####
# A special case for GSM Network interface.
# Don't remove/change the settings, they will cause undefined
behaviour
# of LCR. It uses the loopback interface as defined in
options.conf.
# You may add 'extension' and 'msn' keywords to turn all your
subscribers
# in you GSM network to internal 'extensions'.
# The MSN numbers will equal the subscriber number.
[GSM]
gsm-bs
nt
layer1hold no
layer2hold no
tones yes
earlyb no
channel-in free
channel-out any
nodtmf
```