Universidad de Granada

ESTUDIOS DE INGENIERÍA DE TELECOMUNICACIÓN

PROYECTO FIN DE CARRERA

# Prototipo de estación base GSM usando OpenBTS

CURSO 2014/2015

Alejandro González Garrido

El tribunal constituido para la evaluación del proyecto final de carrera titulado:

**Prototipo de estación base GSM usando OpenBTS**

Realizado por el alumno: **Alejandro González Garrido**

Y dirigido por los tutores: **Jorge Navarro Ortiz** y **José Carlos Segura Luna**

Ha resuelto asignarle la calificación de:

- SOBRESALIENTE (9 - 10 puntos)
- NOTABLE (7 - 8.9 puntos)
- APROBADO (5 - 6.9 puntos)
- SUSPENSO

Con la nota: puntos.

El Presidente:

El Secretario:

El Vocal:

Granada, a de de 2015

D. Jorge Navarro Ortiz y D. José Carlos Segura Luna, profesores del Departamento de Teoría de la Señal, Telemática y Comunicaciones de la Universidad de Granada, como directores del Proyecto Fin de Carrera de D. Alejandro González Garrido

Informan, que el presente trabajo, titulado:

*Prototipo de estación base GSM usando OpenBTS*

Ha sido realizado y redactado por el mencionado alumno bajo nuestra dirección, y con esta fecha se autoriza a su presentación.

Granada, a de de 2015

Fdo. Jorge Navarro Ortiz y José Carlos Segura Luna.

Los abajo firmantes autorizan a que la presente copia de Proyecto Fin de Carrera se ubique en la biblioteca del centro y/o departamento para ser libremente consultada por las personas que lo deseen.

Granada, a de de 2015

Fdo. Jorge Navarro Ortiz y José Carlos Segura Luna

Fdo. Alejandro González Garrido

Universidad de Granada

ESTUDIOS DE INGENIERIA DE TELECOMUNICACIÓN

# Prototipo de estación base GSM usando OpenBTS


REALIZADO POR:

Alejandro González Garrido

DIRIGIDO POR:

Jorge Navarro Ortiz y José Carlos Segura Luna

DEPARTAMENTO:

Teoría de la Señal, Telemática y Comunicaciones.

*A mi padre*

# PROTOTIPO DE ESTACIÓN BASE GSM USANDO OPENBTS.

## PALABRAS CLAVE

GSM, Radio definida por software, OpenBTS, SIP, Asterisk, Voz sobre IP, Modulación GMSK, telefonía móvil, 2G, OsmocomBB.

## RESUMEN

Según los últimos cálculos de la UIT, la red 2G representa más de dos tercios de los aproximadamente 7.000 millones de abonos móviles celulares del mundo, es decir unos 4.600 millones de usuarios en el mundo. Esto quiere decir que, aunque actualmente está en fase de definición la quinta generación móvil, la gran mayoría de los usuarios mundiales actualmente utilizan la red GSM. A pesar de haber sido desplegada desde comienzos de los años 90, GSM aún está muy presente en el mercado y sigue siendo una tecnología muy utilizada.

El presente proyecto pretende desarrollar una estación base de telefonía móvil GSM haciendo uso de un equipo de radio definida por software y la plataforma OpenBTS, permitiendo desplegar una red de telefonía de bajo coste con múltiples utilidades, desde docencia hasta comunicaciones en zonas remotas.

# GSM BASE STATION PROTOTYPE USING OPENBTS.


## KEYWORDS

GSM, Software defined radio, OpenBTS, SIP, Asterisk, voice over IP, GMSK modulation, mobile telephony, 2G, OsmocomBB.


## ABSTRACT


According to the last estimation of the ITU, 2G networks represent more than two thirds of the approximately seven billions of mobile subscriptions in the world, i.e. about 4.6 billions of users in the world. This means that, when the fifth generation of mobile communications is being defined, most of the mobile subscribers are still using GSM networks whose rollout started in the 90s, proving that there is still market for this technology.

The present project aims at developing a GSM base station using software defined radio equipment and the OpenBTS platform, allowing us to deploy a low cost mobile network with multiple applications, from teaching to communications in remote areas.

# AGRADECIMIENTOS

Me gustaría aprovechar esta oportunidad para agradecer a algunas personas por su apoyo y consejos durante la realización del proyecto. En primer lugar a mis tutores, José Carlos y Jorge, por darme la oportunidad de realizar este proyecto ya que gracias a él he conseguido un puesto de trabajo en las oficinas de Nokia Solutions and Networks S.L el cual está íntimamente relacionado con lo desarrollado aquí. También agradecerles el preocuparse de cualquier necesidad que he tenido para poder completarlo.

Para terminar, también agradecer a todas aquellas personas que no han intervenido directamente en el desarrollo del mismo, pero que sin su apoyo nada de lo conseguido durante estos cinco años de carrera hubiera sido posible, mi madre Ángeles, mi hermano Arturo, mis abuelos y mis tíos y primos, ya que entre todos han conseguido que llegue hasta donde he llegado.

Mi más sincero agradecimiento a todos.

# CONTENIDO

**PROTOTIPO DE ESTACIÓN BASE GSM USANDO OPENBTS. IX**

**PALABRAS CLAVE IX**
**RESUMEN IX**

**GSM BASE STATION PROTOTYPE USING OPENBTS. X**

**KEYWORDS X**
**ABSTRACT X**

**AGRADECIMIENTOS XI**

**CONTENIDO 12**

**LISTA DE FIGURAS 15**

**GLOSARIO DE TÉRMINOS 19**

**1. INTRODUCCIÓN 22**

**1.1 COMUNICACIONES MÓVILES 22**
**1.2 MOTIVACIÓN DEL PROYECTO 22**
**1.3 OBJETIVOS 23**
**1.4 ESTRUCTURA DEL DOCUMENTO 23**

**2. RESUMEN DEL ESTÁNDAR GSM 24**

**2.1 INTRODUCCIÓN 24**
**2.2 ARQUITECTURA 28**
2.2.1 LA ESTACIÓN MÓVIL, MS: 28
2.2.2 SUBSISTEMA DE ESTACIÓN BASE BSS: 30
2.2.3 SUBSISTEMA DE RED Y CONMUTACIÓN, NSS: 30
2.2.4 SUBSISTEMA DE OPERACIÓN Y MANTENIMIENTO, OSS: 31
**2.3 INTERFACES DEL SISTEMA GSM 32**
2.3.1 CAPA FÍSICA DEL ENLACE RADIO 32
2.3.2 CAPA ENLACE DE LA INTERFAZ UM 39
**2.4 FUNCIONAMIENTO DEL SISTEMA GSM 41**
2.4.1 SELECCIÓN DE UNA CELDA 41
2.4.2 ACCESO A LA RED 42
2.4.3 REALIZACIÓN DE LLAMADAS 42
2.4.4 ENVÍO Y RECEPCIÓN DE SMS 45
2.4.5 SEGURIDAD EN GSM 45
**2.5 SISTEMA GPRS 47**

**3. SISTEMA PROPUESTO 49**

**3.1 ARQUITECTURA E INTERFACES DE LA RED MÓVIL 49**

3.1.1 COMPARATIVA CON LA RED ACTUAL GSM 49
**3.2 DESCRIPCIÓN HARDWARE 50**
3.2.1 ESTACIÓN MÓVIL 50
3.2.3 SERVIDOR LINUX 51
3.2.4 EQUIPO SDR 51
**3.3 OPENBTS 52**
3.3.1 TRANSCEIVER 52
3.3.2 OPENBTS 53
3.3.3 SIPAUTHSERVE 53
3.3.4 NODEMANAGER 54
3.3.5 SMQUEUE 55
3.3.6 OPENBTSCLI 55
**3.4 ASTERISK 57**
3.4.1 INTRODUCCIÓN 57
3.4.2 GESTIÓN DE USUARIOS 57
3.4.3 PLAN DE LLAMADAS 59
**3.5 SISTEMA OSMOCOMBB 61**

**4. RESULTADOS OBTENIDOS 65**

**4.1 ANÁLISIS DE LOS CANALES EN USO EN LA ZONA DE TEST 65**
4.1.1 BANDA GSM900 66
4.1.2 BANDA DCS1800 67
**4.2 EQUIPO UTILIZADO PARA OBTENER LAS DIFERENTES MEDIDAS 67**
4.2.1 ANALIZADOR VECTORIAL 67
**4.3 ANÁLISIS DE LOS MENSAJES INTERCAMBIADOS ENTRE TODOS LOS SISTEMAS 81**
4.3.1 MENSAJES PERIÓDICOS DE LA BTS 81
4.3.2 CONEXIÓN DE UN MÓVIL A LA RED GSM 85
4.3.3 REALIZACIÓN DE LLAMADAS ENTRE DOS MÓVILES CONECTADOS A OPENBTS 94
4.3.4 ANÁLISIS DE LA CALIDAD DE LA LLAMADA 110
4.3.5 ENVÍO DE SMS 111

**5. APLICACIONES 114**

**5.1 PRESUPUESTO DE UNA INSTALACIÓN 114**
**5.2 ENSEÑANZA EN LABORATORIO DE COMUNICACIONES. 115**
**5.3 TELEFONÍA EN ZONAS RURALES. 116**
**5.4 COMUNICACIONES TRAS DESASTRES NATURALES 117**

**6. CONCLUSIONES Y TRABAJO FUTURO 119**

**ANEXO 1. INSTALACIÓN DEL EQUIPO SDR EN EL SERVIDOR 120**

**ANEXO 2. INSTALACIÓN Y CONFIGURACIÓN DE OPENBTS 125**

**COMENZAREMOS POR INSTALAR GIT. 125**
**INSTALACIÓN DE OPENBTS. 125**
**CONFIGURACIÓN DE OPENBTS. 126**

**ANEXO 3. INSTALACIÓN DE OSMOCOM-BB 127**

**HARDWARE** **127**
**SOFTWARE** **127**

**ANEXO 4. OBTENCIÓN DEL IMSI DE UNA TARJETA SIM** **132**

**ANEXO 5. LEGISLACIÓN DE EMISIONES RADIOELÉCTRICAS EN ESPAÑA** **136**

**BIBLIOGRAFÍA** **142**

**ÍNDICE** **144**

# LISTA DE FIGURAS

1. CRECIMIENTO DE LÍNAS MÓVILES EN ESPAÑA ..... 22
2. LOGOTIPO DEL ESTÁNDAR GSM [2] ..... 24
3. TABLA COMPARATIVA REDES PRIMERA GENERACIÓN [3] ..... 25
4. PRIMERAS NOTICIAS SOBRE GSM EN ESPAÑA. [5] ..... 25
5. NOTICIA DEL DESPLIEGUE DE LA RED GSM EN ESPAÑA [6] ..... 26
6. ARQUITECTURA RED GSM+GPRS [7] ..... 28
7. PRIMEROS MÓVILES GSM DE TELEFÓNICA [6] ..... 28
8. ARQUITECTURA DEL EQUIPO DEL ABONADO [3] ..... 29
9.TAMAÑOS DE SIM. ESTÁNDAR, MINI, MICRO Y NANO [8] ..... 29
10. ARQUITECTURA SIM 2G/3G [9] ..... 29
11. FLEXI BTS DE NOKIA CON 3 SECTORES [10] ..... 30
12. EJEMPLO DE CONMUTADOR GSM DE ERICSON ..... 31
13. EJEMPLO INTERFAZ DE CONFIGURACIÓN DE UNA BTS NOKIA ..... 32
14. DIAGRAMA DEL MODULADOR GMSK ..... 33
15. CONSTELACION GMSK DE GSM ..... 34
16. COMPARACIÓN DE VARIACIÓN DE FRECUENCIA Y FASE EN MSK Y GMSK ..... 34
17. ESPECTRO GMSK DE UNA SEÑAL GSM ..... 35
18. EJEMPLO DE ENTRELAZADO POR MATRIZ ..... 36
19. TABLA DE CODIFICACION CANALES EN GSM ..... 37
20. ESPECTRO USADO POR GSM ..... 37
21. CANALIZACIÓN DE LA BANDA GSM900 ..... 38
22. DIVISION TEMPORAL DE CADA CANAL GSM [11] ..... 38
23. DISTRIBUCIÓN EN MULTITRAMA DE LOS DIFERENTES CANALES DE CONTROL ..... 39
24. DISTRIBUCIÓN DE CANALES DE TRÁFICO ..... 40
25. MÁSCARA DEL TIEMPO DE GUARDA DE UNA RÁFAGA ..... 40
26. RÁFAGA NORMAL ..... 41
27. ILUSTRACIÓN DE UN SISTEMA CELULAR CON 4 CELDAS [12] ..... 41
28. PROCESO DE IMSI ATTACH COMPLETO ..... 42
29. PROCESO DE REALIZACIÓN DE LLAMADA ORIGINADA EN MÓVIL ..... 43
30. EJEMPLO DE ENVÍO DE MENSAJE DE PAGING POR LA ZONA DE COBERTURA DEL MÓVIL ..... 44
31. MENSAJES TRANSMITIDOS PARA ESTABLECER UNA LLAMANDA HACIA UN MÓVIL ..... 44
32. PROCEDIMIENTO DE AUTENTICACION EN UNA RED GSM ..... 46
33. PROCEDIMIENTO DE CIFRADO DE LAS COMUNICACIONES ..... 46
34. ARQUITECTURA GPRS ..... 47
35. MAPEO DE ASIGNACION DE TS PARA GPRS ..... 48
36. LOGOTIPO DE LA IMPLEMENTACIÓN COMERCIAL DE OPENBTS [13] ..... 49
37. ARQUITECTURA DESARROLLADA EN OPENBTS [14] ..... 49
38. TABLA COMPARATIVA ENTRE GSM CONVENCIONAL Y OPENBTS ..... 50
39. TABLA DE DISPOSITOS MÓVILES UTILIZADOS EN EL PROTOTIPO ..... 50
40. TABLA TARJETAS SIM DE PRUEBA ..... 51
41. EQUIPO SDR UTILIZADO PARA EL PROTOTIPO ..... 51
42. POSICION DE ANTENAS TX/RX PARA MINIMIZAR POSIBLES INTERFERENCIAS ..... 52
43. ARQUITECTURA DE OPENBTS ..... 52
44. EJEMPLO DE ABONADOS EN LA BASE DE DATOS ..... 55
45. ASTERISK Y SU NUBE DE POSIBILIDADES DE INTERCONEXIÓN ..... 57
46. SERVICIO TRONCAL SIP CONRATADO ..... 58
47. DETALLES DEL LOG DE CONEXION AL SERVCIO TRONCAL ..... 59

48. Terminales liunx para el control del sistema osmocombb ..... 61
49. pagina web del ministerio con información de las antenas de telefonía móvil instaladas cerca de la etsiit ..... 65
50. Detalle de las antenas cercanas a la etsiit ..... 66
51. Operadores y banda asignada en gsm900 ..... 66
52. Montaje para las medidas del canal GSM ..... 68
53. Potencia del canal en uso ..... 69
54. Potencia en canales adyacentes al nuestro ..... 70
55. Ancho de banda ocupado por la señal gsm ..... 71
56. Espectro GSM según estándar ..... 71
57. Niveles de potencia para la máscara de emisión ..... 72
58. Máscara del espectro de emisión ..... 72
59. Potencia de transmisión en DCS1800 ..... 73
60. Potencia en canales adyacentes ..... 73
61. Ancho de banda ocupado ..... 74
62. Máscara del espectro de emisión ..... 74
63. Agilent 89600 VSA ..... 75
64. constelación gmsk en vsa ..... 75
65. error de vector IQ en constelación ..... 76
66. 8 Time Slots de C0 ..... 76
67. espectro gsm ..... 77
68. Resumen medidas gsm en VSA ..... 77
69. Ráfaga gsm ..... 78
70. constelación gmsk en gsm900 y dcs1800 ..... 78
71. Errores en medidas ..... 79
72. Slots temporales de una portadora GSM ..... 79
73. Ráfagas en un Slot Temporal ..... 80
74. Señal temporal del enlace ascendente 1 y 2 llamadas Simultáneas ..... 80
75. Señal temporal del enlace ascendente 3 y 4 llamadas simultáneas ..... 81
76. Mensajes periódicos de la BTS ..... 81
77. Mensajes periódicos de la BTS al MS ..... 82
78. Cabecera GSMTAP ..... 82
79. Mensaje system information type 1 ..... 83
80. Mensaje System Information Type 2 ..... 83
81. Mensaje System Information Type 3 ..... 84
82. Mensaje system information type 4 ..... 85
83. Mensajes intercambiados para el registro de un MS en la red GSM ..... 85
84. Mensajes de conexión a la red de un móvil ..... 86
85. Datos de un mensaje de información del sistema tipo 5 ..... 86
86. Mensaje de información del sistema tipo 6 ..... 87
87. cabecera mensaje de asignación de canal ..... 87
88. Mensaje de asignación de canal de tráfico a un móvil ..... 87
89. Mensaje del móvil de actualización de localización ..... 88
90. respuesta a la actualización de localización por parte de la BTS ..... 89
91. Mensaje de petición de identidad ..... 89
92. Intento de registro en la centralita de llamadas ..... 90
93. Informe de medidas de calidad del enlace MS-BTS ..... 90
94. Respuesta a la petición de identidad ..... 91
95. Registro en el core de la red ..... 91
96. Respuesta al intento de registro no autorizado por el core ..... 91
97. Mensaje de Petición de autorización cifrada ..... 92
98. Mensajes de registro satisfactorio en asterisk ..... 92

99. MENSAJE DE RESPUESTA A LA PETICIÓN DE AUTORIZACIÓN CIFRADA ..... 92
100. MENSAJE DE PETICIÓN DE REGISTRO EN ASTERISK ..... 92
101. RESPUES DE REGISTRO ACEPTADO EN CENTRALITA ..... 93
102. MENSAJE DE ACTUALIZACIÓN DE LA LOCALIZACIÓN ACEPTADO ..... 93
103. DETALLE DEL MENSAJE DE ACTUALIZACIÓN DE LA LOCALIZACIÓN ACEPTADA ..... 93
104.MENSAJE DEL MÓVIL DE PETICIÓN DE ACCESO PARA LLAMADA ..... 95
105. MENSAJE DE PETICIÓN DE CANAL DE TRÁFICO ..... 95
106. MENSAJE BTS-MS ACEPTANDO LA PETICIÓN DEL CANAL DE COMUNICACIONES ..... 95
107. MENSAJE DE CANCELACIÓN DE TRANSMISIÓN GPRS ..... 96
108. MENSAJE DE INTENTO DE LLAMADA POR ASTERISK ..... 96
109. MENSAJE DE MS-BTS PARA PREPARAR LA LLAMADA ..... 96
110. MENSAJE SIP PARA REALIZAR LA LLAMADA DE LA BTS A ASTERISK ..... 97
111. MENSAJE DE ASTERISK A SIPAUTHSERVE PARA OBTENER EL IMSI DE UN NÚMERO ..... 97
112. MENSAJE DE RESPUESTA DE LA PETICIÓN DEL IMSI DE UN NÚMERO ..... 98
113. MENSAJE DE ASTERISK A LA BTS PARA QUE REALICE BUSQUE AL MS AL QUE VA DESTINADA LA LLAMADA ..... 98
114. MENSAJES PARA INDICAR EL INICIO DE LLAMADA BTS-MS Y MS-BTS ..... 99
115. MENSAJE DE LA BTS A LOS MS PARA INDICAR LA LLEGADA DE UNA LLAMADA. ..... 99
116. MENSAJE DE ASIGNACIÓN DEL CANAL FÍSICO PARA CURSAR LA LLAMADA. BTS-MS ..... 99
117. DETALLE MENSAJE DE ASIGNACIÓN DE TS PARA CURSAR LA LLAMADA ..... 99
118. CONFIRMACIÓN DE LA ASIGNACIÓN DEL CANAL ..... 99
119. CONFIRMACIÓN DEL MS DE LA ASIGNACIÓN DE TS PARA LA LLAMADA ..... 100
120. MENSAJES DE RESPUESTA A LA INDICACIÓN DE LLAMADA ..... 100
121. MENSAJE CON NÚMERO LLAMANTE ..... 100
122. DETALLE DEL MENSAJE CON NÚMERO LLAMANTE ..... 100
123. MENSAJE DE CONFIRMACIÓN DE RECEPCIÓN DE LLAMADA ..... 100
124. DETALLE DEL MENSAJE DE CONFIRMACIÓN DE RECEPCIÓN DE LLAMADA ..... 101
125. MENSAJES DE ASIGNACIÓNDE CANAL PARA RECEPCIÓN DE LLAMADA ..... 101
126. DETALLE DE LA ASIGNACIÓN DE TS POR PARTE DE LA BTS ..... 101
127. CONFIRMACIÓN DE LA ASIGNACIÓN DE CANAL ..... 101
128. DETALLE DEL MENSAJE DE CONFIRMACIÓN ..... 102
129. MENSAJE DE ALERTA DE LA BTS AL MS LLAMADO ..... 102
130.DETALLE DEL MENSAJE DE ALERTA ..... 102
131. MENSAJES SIP DE LLAMADA EN PROCESO ..... 102
132. MENSAJE DE ASTERISK A LA BTS CON DESTINO EL MÓVIL LLAMADO ..... 103
133. MENSAJE ENTRE BTS DE PARTE DEL MÓVIL LLAMANTE HACIA ASTERISK ..... 103
134. MENSJA DE ALERTA DE LA BTS AL MÓVIL LLAMANTE ..... 103
135. MENSJAES QUE CONFIRMAN CURSAR LA LLAMADA ..... 104
136. MENSAJE DE CONFIRMACIÓN DE DESCOLGADO DEL TELÉFONO ..... 104
137. MENSAJE SIP DE OK AL INVITE ..... 104
138. CONFIRMACIÓN DEL RINGING ..... 104
139. MENSAJE DE OK AL INVITE DE LLAMANTE ..... 105
140. MENSAJE DE CONFIRMACIÓN DEL MENSAJE RINGING ..... 105
141. CONFIRMACIÓN DE LA COMUNICACIÓN DE LA BTS AL LLAMANTE ..... 105
142. CONFIRMACIÓN DE LA LLAMADA DE LA BTS AL MS LLAMADO ..... 105
143. CONFIRMACIÓN DE LA LLAMADA DEL LLAMANTE A LA BTS ..... 106
144. INTERCAMBIO DE MENSAJES AL FINALIZAR UNA LLAMADA ..... 106
145. LLAMANTE CUELGA EL MÓVIL ..... 106
146. MENSAJE DE CIERRE DE LA CONEXIÓN ENTRE BTS Y ASTERISK ..... 107
147. CONFIRMACIÓN POR PARTE DE ASTERISK AL CIERRE DE LA CONEXÍON. ..... 107
148. INDICACIÓN DE ASTERISK A LA BTS DEL CIERRE DE LA CONVERSACIÓN POR PARTE DEL LLAMANTE. ..... 107
149. CONFIRMACIÓN DE LA BTS A ASTERISK DE LA RECEPCIÓN DEL MENSAJE DE CIERRE DE LA COMUNICACIÓN .. 108
150. MENSAJE DE LA BTS AL MÓVIL LLAMANTE DE QUE HA TERMINADO LA COMUNICACIÓN. ..... 108

151. MENSAJE DE LA BTS AL LLAMADO PARA LA DESCONEXIÓN DE LA RED ..... 108
152. CONFIRMACIÓN DEL MÓVIL LLAMANTE DE LA FINALIZACIÓN DE LA LLAMADA ..... 108
153. MENSAJE DEL MÓVIL LLAMADO A LA BTS PARA INDICAR EL FIN DE LA COMUNICACIÓN ..... 109
154. MENSAJES PARA DEJAR LIBRE EL CANAL RADIO ..... 109
155. INDICACION DE LA BTS AL LLAMANTE DE QUE SE VA A LIBERAR EL CANAL RADIO ..... 109
156. CONFIRMACIÓN DE LA BTS AL MÓVIL LLAMAO DE LA LIBERALICACIÓN DEL CIRCUITO DE LA LLAMADA ..... 109
157. MENSAJE DE LIBERACIÓN DEL CANAL RADIO POR PARTE DEL MOVIL LLAMADO ..... 109
158. DETALLE DEL MENSAJE DE LA LIBERACIÓN DEL CANAL RADIO. ..... 110
159. ESTADÍSTICAS DE LAS MEDIDAS DE LOS PARÁMETROS DE LA CONVERSACIÓN. ..... 110
160. EVOLUCIÓN DEL JITTER EN LA LLAMADA ..... 110
161. MENSAJES INTERCAMBIADOS AL ENVIAR Y RECIBIR UN SMS ..... 111
162. MENSAJES RESPONSABLES DEL ENVÍO DE UN SMS ..... 111
163. MENSJAE ENTRE MS Y BTS CON EL ENVÍO DE UN SMS ..... 111
164. MENSAJE SIP ENTRE LA BTS Y SMQUEUE ..... 112
165. MENSAJE SIP ENTRE SMQUEUE Y EL DESTINO ..... 112
166. MENSAJE DE LA BTS AL MS CON LA CONFIRMACIÓN DE LA RECEPCIÓN DEL SMS ..... 112
167. DETALLE DE LA CONFIRMACIÓN DE RECEPCIÓN DEL SMS ..... 112
168. MENSAJE ENTRE ELEMENTO DE LA RED Y LA BTS ..... 113
169. DETALLE DEL MENSAJE SMS ENVÍADO POR SIP ..... 113
170. MENSAJE DE LA BTS AL MÓVIL CON EL SMS ..... 113
171. DETALLE DEL MENSAJE ENVIADO POR LA BTS AL MS CON EL SMS ..... 113
172. INSTALACIÓN DE LABORATORIO ..... 114
173. PRESUPUESTO DE UNA INSTALACIÓN DE LABORATORIO ..... 114
174. PRESUPUESTO DE UNAS INSTALACIÓN EN CAMPO ..... 115
175. HTTP://WWW.VNL.IN EJEMPLO DE NEGOCIO BASADO EN LAS MICROTELECOM ..... 116
176. OPENBTS DESPLEGADA EN LA SELVA ..... 117
177. EJEMPLO DE INFRAESTRUCTURA GSM PARA EMERGENCIAS ..... 118
178. OPENCELL SERIES DE RANGE NETWORKS ..... 118
179. COMPILACIÓN COMPLETADA ..... 129
180. COMPILADOR ARM DISPONIBLE ..... 129
181. LINEA A MODIFICAR PARA PERMITIR LA TRANSMISIÓN ..... 130
182. FASES PARAR LA MEDICIÓN DE UNA INSTALACIÓN ..... 137

# GLOSARIO DE TÉRMINOS

**ACP:** Potencia en canales adyacentes al principal, también se refiere a esta medida como relación de potencia en canales adyacentes, ACPR de sus siglas en inglés o índice de fuga en canales adyacentes, ACLR de sus siglas en inglés.

**Ancho de banda ocupado:** Definición de medida RF que nos devuelve el ancho de banda ocupado por una estación GSM, calculando la potencia en toda la banda y obteniéndo dónde está el 99% de esa potencia.

**ARFCN:** Número de frecuencia absoluta, o de las siglas *Absolute Radio-Frecuency Chanel Number*. Es un número que identifica cada canal físico de 200Khz de ancho en las bandas de 900Mhz y de 1800Mhz.

**Asterisk:** Software que implementa una centralita privada, o PBX, para llamadas de voz sobre IP.

**BCCH:** De sus siglas en inglés, *Broadcast Common Channel*, canal lógico de GSM para la difusión de información relativa de la red a los móviles que hay en su zona de cobertura.

**BSC:** De sus siglas en inglés, *Base Station Controller*. Equipo encargado de controlar las BTS de su zona e interconectarlas con el conmutador de llamadas.

**BTS:** De sus siglas en inglés, *Base Station Transceiver*. Equipo encargado de la comunicación directa entre la red de telefonía y los teléfonos móviles.

**DCS1800:** Nombre de la banda GSM desplegada en la zona de 1800Mhz del espectro.

**Ecualización del canal:** Técnica por la cual, el receptor de una señal radio, a partir de ciertos bits conocidos entre emisor y receptor, es capaz de estimar el comportamiento del canal y proceder a la minimización de los posibles errores encontrados en la señal, mejorando la relación señal-ruido mínima para realizar una comunicación.

**FACCH:** De sus siglas en inglés, *Fast Associated Common CHannel*, canal rápido asociado a un canal de tráfico. Usado por BTS y móvil en caso de necesitar un traspaso de llamada o para llamadas de emergencia.

**FDD**: De sus siglas en inglés, *Frequency-Division Duplexing*, duplexado por división de frecuencia, es decir, uso de bandas diferentes para el enlace ascendente y para el descendente permitiendo una comunicación bidireccional a la vez.

**FDMA:** Acceso múltiple por división de frecuencia, acrónimo de *Frequency Division Multiple Access*, división de una banda de frecuencias en diferentes canales contiguos, cada uno usado por un emisor diferente.

**GMSK:** Modulación digital por desplazamiento mínimo gaussiano, de sus siglas en inglés, *Gaussian Minimun Shift Keying*. La señal digital, previa a la modulación, se forma primero con un filtro gaussiano, lo que tiene la ventaja de reducir la potencia de banda lateral y, a su vez, reduce la interferencia fuera de banda.

**GPRS:** Es el estándar utilizado para disponer de una red de paquetes sobre GSM. Las siglas vienen de *General Packet Radio Service*.

**GSM:** Estándar de comunicaciones móviles celulares de segunda generación.

**GSM900:** Nombre para la banda de 900Mhz que hace uso del estándar GSM.

**GSMTAP:** Cabecera añadida a las tramas radio Um para ser transportadas vía paquetes IP/UDP. Utilizado para analizar dichas tramas mediante algún software compatible.

**HLR:** Registro de localización local, del inglés *Home Locator Register*. Utilizado para almacenar la localización de los móviles, necesaria en caso de tener que enviar un aviso de llamada entrante.

**IMSI**: Es el acrónimo de *International Mobile Subscriber Identity* (Identidad Internacional del Abonado a un Móvil). Es un código asociado a la tarjeta SIM del abonado y único en el mundo que permite la identificación del usuario en una red GSM y UMTS.

**Interferencia intersimbólica**: Es la perturbación de la señal recibida que se manifiesta mediante ensanchamiento temporal, y el solapamiento de pulsos individuales hasta el punto de que el receptor puede no distinguir correctamente entre cambios de estado.

**MSC:** *Mobile Switching Centre*, o Centro de Conmutación de Servicios Móviles. Es el equipo encargado de realizar la interconexión de circuitos entre diferentes usuarios de la red móvil, o entre usuarios de la red móvil y la red fija.

**OpenBTS:** Software que implementa toda la funcionalidad de una BTS+BSC del estándar GSM.

**PAGCH:** Canal lógico GSM para el aviso de llegada de llamadas.

**PAGING:** Mensaje enviado por el canal lógico PAGCH en el que la BTS indica al móvil la llegada de una llamada entrante.

**Potencia del canal:** Medida que se corresponde al 99% de la potencia RF de un canal GSM frente al resto de la banda.

**RACH:** Canal de acceso común de los móviles a la red. En él indican la necesidad de un canal dedicado para comenzar una llamada.

**Ráfaga:** Conjunto de bits transmitidos durante un *slot* temporal.

**Red celular:** Red de comunicaciones en la cual la cobertura está basada en un conjunto de celdas, de tal forma que sea transparente para el usuario el cambio de una celda a otra.

**SACCH:** Canal lógico de baja velocidad o *Slow Associated Common Channel*. Está asociado a un canal de tráfico y transmite información relativa al control de potencia para el móvil y el avance temporal de las tramas.

**SCH:** De sus siglas en inglés, *Syncronization Channel*. Canal lógico por el que la BTS informa a los móviles acerca del avance temporal de las tramas, el código de identificación de la BTS y una secuencia de entrenamiento para la ecualización del canal radio.

**SDR:** Equipo de radio definido por software, o *Software Defined Radio*. Es el elemento que transforma las tramas I/Q que se generan por software y las convierte en una radiación electromagnética, y viceversa, recibe una señal electromagnética, muestrea la señal y la envía a un ordenador para su procesado.

**SIM:** Tarjeta inteligente necesaria para acceder a una red GSM. Es el acrónimo de *Subscriber Identity Module*, contiene diversa información, donde la más importante es el IMSI, la clave de autenticación (Ki) y la identificación de área local (LAI).

**SMS:** Servicio de Mensajes Cortos, *Short Message Service*, servicio adicional de la red GSM que permite el intercambio de mensajes de texto cortos.

**TCH:** Canal de tráfico del usuario. Es un canal lógico GSM por el que se transmite la señalización del usuario y posteriormente la voz al realizar una llamada.

**TDMA:** Técnica de acceso al medio por división temporal. *Time Division Medium Access*. Consiste en dividir el tiempo en diferentes ranuras o *slot* temporales de corta duración, y asignar cada uno a un usuario, de forma que el usuario que necesite transmitir o recibir un dato debe esperar a su turno para enviar o recibir.

***Timeslot*:** Ranura temporal utilizada con la técnica TDMA. En GSM cada canal radio se divide en 8 ranuras, siendo la correspondiente al canal 0 y ranura 0 dedicada a mensajes de control de la red y el resto para transmisión de datos del abonado.

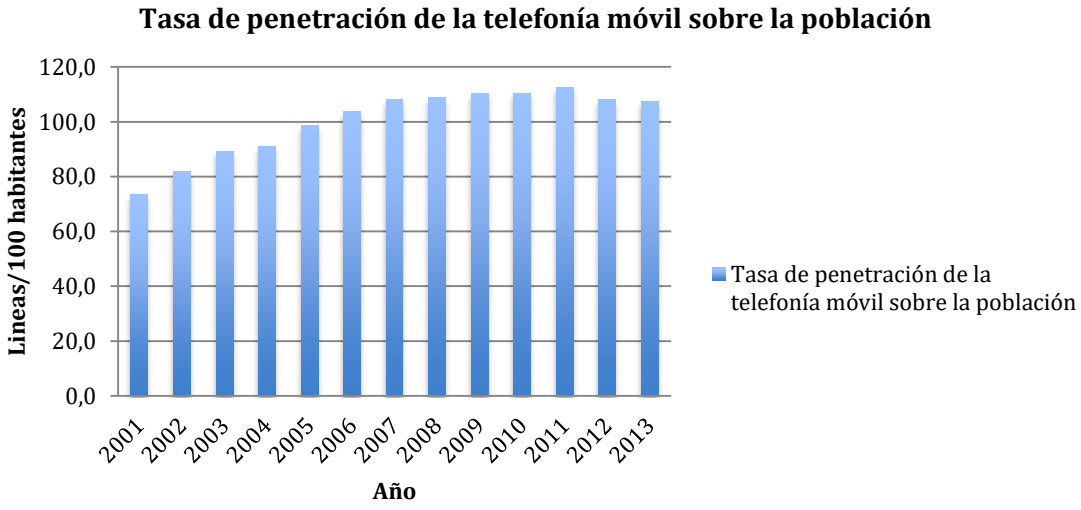
**VoIP:** Tecnología por la cual una llamada se digitaliza y encapsula en tramas para una red IP, por conmutación de paquetes y no por conmutación de circuitos como se viene haciendo tradicionalmente. Suele implicar el uso del protocolo SIP para la señalización del usuario y del protocolo RTP para el tráfico de la voz.

# 1. INTRODUCCIÓN

## 1.1 COMUNICACIONES MÓVILES

La sociedad de la información es aquella en la cual las tecnologías que facilitan la creación, distribución y manipulación de la información juegan un papel esencial en las actividades sociales, culturales y económicas. La forma en que hacemos compras, interactuamos con la banca, el acceso a servicios públicos y un largo etcétera son ejemplos actuales que definen muy bien que estamos en la sociedad de la información.

La telefonía móvil ha jugado un papel importante ya que a día de hoy es posible realizar casi todas esas tareas desde el terminal móvil, gracias a la posibilidad de acceso a Internet que ofrecen. Actualmente, hay casi tantas líneas móviles como habitantes en el planeta. En el caso de España nos quedamos con las cifras del informe anual de la Comisión del Mercado y la Competencia [1]:




**1. CRECIMIENTO DE LÍNAS MÓVILES EN ESPAÑA**

Como se puede observar en el gráfico anterior, al comienzo del año 2014 había más líneas móviles en España que habitantes, tendencia seguida desde el año 2006.

Las grandes empresas proveedoras de servicios de telefonía móvil son las que pueden permitirse realizar el despliegue a gran escala de sus redes, estando controladas por ellas las zonas de interés comercial, basadas en estudios de densidad de población. Generalmente las zonas más pobladas son las que mejores servicios disponen, dejando las zonas más aisladas carentes de servicios, o muy limitados en cuanto a capacidad.

## 1.2 MOTIVACIÓN DEL PROYECTO

El presente proyecto trata de ofrecer una solución de bajo coste para el despliegue de una red celular basada en el estándar GSM (*Global System for Mobile communications*) + GPRS (*General Packet Radio Service*), como plataforma docente para asignaturas de comunicaciones móviles.

Como se podrá ver en el capítulo dos, sobre el estándar GSM, la arquitectura actual implica sistemas cerrados, con poca flexibilidad y un alto coste económico.

La reducción de costes de los equipos radio definidos por software, junto con el aumento de las prestaciones de los procesadores, están marcando una nueva tendencia en los sistemas de

comunicaciones. Esto permite diseñar cualquier servicio de comunicaciones a partir de un pequeño equipo hardware, estando el resto del sistema definido por el software que ejecutará un procesador de propósito general.

Gracias a estos factores, con poco presupuesto se puede desplegar una pequeña red celular propia para prestar servicios de voz y datos. El proyecto desarrollado en este documento es un ejemplo de dicha tecnología.

## 1.3 OBJETIVOS

El principal objetivo de este proyecto es desplegar una estación base de GSM+GPRS de forma que dos terminales móviles puedan conectarse a ella, realizar llamadas entre ellos, enviar y recibir SMS y tener acceso a Internet haciendo uso del sistema abierto OpenBTS, un PC y un equipo radio SDR.

Los objetivos secundarios son:

- Poner a prueba, en base al estándar GSM, las capacidades del equipo SDR para trabajar como estación base GSM.
- Realizar un estudio sobre el intercambio de información dentro de una red GSM basada en OpenBTS.

## 1.4 ESTRUCTURA DEL DOCUMENTO

El presente documento se divide en seis capítulos y cinco anexos. El capítulo uno realiza una introducción a las comunicaciones móviles y al proyecto desarrollado. El capítulo dos es un resumen del estándar GSM de forma que el lector pueda conocer los conceptos empleados en el resto del documento. En el siguiente capítulo, el tercero, se hace una descripción completa del prototipo desarrollado como alternativa al actual sistema GSM. En el cuarto capítulo se detallan los diferentes test y pruebas a los que se ha sometido el prototipo en cuestión, junto con la discusión respecto a los requisitos del estándar GSM. En el capítulo cinco hay una pequeña muestra de las posibilidades comerciales de este sistema. El capítulo sexto concluye el trabajo realizado y describe los posibles siguientes pasos para mejorar el sistema.

Para finalizar el documento, se incluyen cinco anexos, una lista de términos utilizados en el documento y las referencias bibliográficas. El primero de los anexos versa sobre el proceso a seguir para la instalación del equipo SDR, es decir, la configuración necesaria en el servidor Linux para una correcta operación del dispositivo. Después, el siguiente anexo explica el proceso de compilación e instalación de OpenBTS. El tercer y cuarto anexo tratan sobre el paquete de aplicaciones OsmocomBB, usadas para analizar las tarjetas SIM utilizadas y para obtener capturas de tráfico de mensajes de la red y el móvil. El penúltimo de los anexos indica cómo averiguar el IMSI de una tarjeta SIM, necesario para dar de alta a los usuarios en OpenBTS. Y los anexos terminan con una descripción de la legislación española en materia de emisiones radioeléctricas en nuestras bandas de interés.

# 2. RESUMEN DEL ESTÁNDAR GSM

**2. LOGOTIPO DEL ESTÁNDAR GSM [2]**

Este segundo capítulo realizará una exposición sobre el estándar GSM, de forma que un lector que no esté familiarizado con dicho estándar pueda entender con facilidad los conceptos utilizados en capítulos posteriores [3] [4].

## 2.1 INTRODUCCIÓN

Todos los sistemas de comunicaciones móviles tienen en común una serie de características, siendo la más importante la libertad de desplazamiento del terminal móvil durante la comunicación y una vez finalizada ésta. Para conseguir esa libertad de movimientos hay dos opciones disponibles: pocas estaciones transmisoras de gran potencia y gran cobertura; o muchas estaciones transmisoras de poca cobertura y menor potencia de transmisión.

El concepto de red celular apareció en los años cuarenta por los laboratorios Bell. En lugar de utilizar un modelo de estaciones base emitiendo elevadas potencias en puntos geográficos dominantes (como lo hace la radio y televisión terrestres en la actualidad) se diseñó una arquitectura con un gran número de pequeños transmisores, cada uno con un área de cobertura menor y transmitiendo menor potencia. Este modelo es más viable para una red de dispositivos móviles ya que la distancia entre cada estación móvil y la estación base es menor, lo que requiere menor potencia transmisora para los dispositivos móviles, que normalmente funcionan a baterías. En este sistema aparece el concepto de reutilización de frecuencias, de forma que cada celda tenga una frecuencia diferente al resto de celdas que están en su entorno para evitar interferencias, pero pudiendo repetirse cuando está fuera de ese entorno. Este planteamiento supone que, si cada vez se hacen menores las células, la capacidad teórica sería ilimitada ya que se conseguiría soportar un mayor número de comunicaciones por kilómetro cuadrado, quedó demostrado que era inviable al no tener la capacidad de gestionar un número ilimitado de celdas.

La posibilidad de movimiento del terminal móvil hace necesaria conocer la localización de los mismos para que puedan recibir llamadas. Para que esto sea posible, el terminal dialoga esporádicamente con las diferentes estaciones base que se encuentran a su alrededor. Por lo tanto, si éste se desplaza por diferentes celdas, el sistema tendrá conocimiento de en qué celda se encuentra. Esta libertad de movimiento hace que el enlace radio entre el terminal móvil y la estación base varíe con el tiempo, por lo que se debe proteger el enlace radio de tal forma que se pueda asegurar un mínimo de calidad en la comunicación en cualquier momento (de 9 a 11 dB de SNR como mínimo según [3]). Los mecanismos que contrarrestan las interferencias, desvanecimientos, distorsión de la señal, etcétera, mejoran en cada generación de sistemas celulares permitiendo umbrales inferiores de SNR.

Los primeros sistemas celulares de comunicaciones móviles 1G fueron sistemas analógicos desarrollados por cada país, o conjunto pequeño de países, por separado e incompatibles entre sí.

Las características de los principales sistemas como son: AMPS (*Advanced Mobile Phone System*), TACS (*Total Access Communications System*), NMT (*Nordiska MobilTelefoni-gruppen*) y NAMTS (*Nippon Automatic Mobile Telephone System*) se resumen en la siguiente tabla:

| **Sistema** | **AMPS** | **TACS** | **NMT** | **NAMTS** |
|---|---|---|---|---|
| **Banda ascendente (MHz)** | 824-849 | 872-905 | 890-915 | 925-940 |
| **Banda descendente (MHz)** | 869-894 | 917-950 | 935-960 | 870-885 |
| **Ancho de canal (KHz)** | 30 | 25 | 12,5 | 25 |
| **Número de canales** | 832 | 1320 | 1999 | 600 |
| **Modulación** | FM | FM | FM | FM |
| **Desviación en frecuencia (KHz)** | 12 | 9,5 | 5 | 5 |
| **Señalización** | FSK | FSK | FSK | FSK |
| **País de origen** | América | Reino Unido | Países escandinavos | Japón |
| **Fin de operación** | Operativo | 26 Enero 2001 | 10 Enero 2008 | No hay información |

**3. TABLA COMPARATIVA REDES PRIMERA GENERACIÓN [3]**

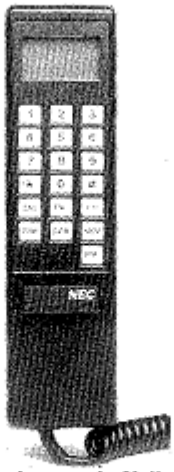
En la tabla anterior se puede observar la disparidad entre los diferentes sistemas de comunicaciones móviles de primera generación.

# PRIMERA DEMOSTRACIÓN PÚBLICA DEL SISTEMA DE TELEFONÍA CELULAR PAN-EUROPEA GSM

Motorola, a través de su División de Infraestructura Celular Europea, realizó la primera demostración pública del sistema de Telefonía Móvil Celular Pan-Europea GSM en Hannover (Alemania), coincidiendo con la celebración de la feria internacional de la electrónica, informática y telecomunicaciones, CeBIT.

Las primeras llamadas del sistema GSM fueron realizadas desde el "stand" de la compañía telefónica alemana Deutsche Bundespost Telekom (DBT) por el ministro federal de Correos y Telecomunicaciones, doctor Christian Schwarz-Schilling, y el presidente del DBT, Helmut Ricke.

Motorola hizo posible la demostración facilitando personal técnico y material de su fabricación para instalar el CeBIT una estación base de transmisión-recepción, software informático para el sistema y un centro de conmutación móvil, así como dos teléfonos móviles digitales GSM, considerados como prototipos de la próxima generación de terminales móviles celulares.



**Comunicaciones más fáciles**

El Groupe Spéciale Mobile (GSM) será el primer sistema pan-europeo de telefonía móvil celular digital. Cuando entre en servicio, cualquier abonado al sistema en un país europeo determinado podrá utilizar su terminal móvil en los restantes países, haciendo realidad la intercomunicabilidad total. Equipos de infraestructura celular Motorola están en servicio ya en toda Europa. El sistema TACS de 900 Megaherzios es operativo en España –donde se denomina TMA 900 A–, Austria y el Reino Unido. Motorola ha recibido también el encargo de poner en marcha sistemas de validación del GSM en España, Alemania y el Reino Unido, y sistemas preoperacionales y operacionales en España, Suecia y el Reino Unido.

Motorola es la compañía líder en el desarrollo, fabricación y suministro de equipos, infraestructura y productos para abonado en los diferentes sistemas de telefonía móvil celular. También diseña, fabrica y comercializa sistemas, componentes y equipos en diferentes campos de la electrónica y las telecomunicaciones, tales como radiocomunicaciones, buscapersonas, semiconductores, electrónica militar, aeroespacial, industrial y para el automóvil, así como equipos para el proceso, tratamiento y transmisión de datos.

**4. PRIMERAS NOTICIAS SOBRE GSM EN ESPAÑA. [5]**

La segunda generación apareció motivada para intentar unificar el sistema de comunicación móvil y para intentar paliar las principales limitaciones de los sistemas de primera generación:

- Limitada capacidad. Por debajo de la demanda del mercado de los sistemas de primera generación.
- Las incompatibilidades entre los diferentes estándares de primera generación hacía imposible el uso del mismo terminal móvil en diferentes países.
- No disponer de mecanismos de control de potencia independientemente de la ubicación del terminal móvil aumenta la interferencia. Si emite con máxima potencia muy cerca de la estación base, produce mucha más interferencia al sistema, que si dispone de un mecanismo de control automático de potencia de forma que emita el mínimo necesario para obtener una comunicación correcta.
- Complejidad creciente de gestión de celdas cada vez más pequeñas.
- Ineficiencia de la transmisión analógica.

El estándar mas conocido de sistema de segunda generación es GSM. Las características principales del sistema GSM eran la buena calidad del servicio, terminales y servicios baratos, *roaming* internacional, eficiencia espectral, compatibilidad RDSI, etc. El servicio comercial del sistema GSM llegó en 1992 como pruebas en la Expo92 en Sevilla y de forma definitiva en 1993.

2 LA VANGUARDIA MARTES, 23 OCTUBRE 1990

PUBLIRREPORTAJE

TELECOMUNICACIONES

# DE LA TELEFONÍA MÓVIL A LA TELEFONÍA PORTÁTIL

A partir de 1993 será introducido en España el Servicio de Telefonía Móvil Digital paneuropeo, que ofrecerá a todos los usuarios del territorio comunitario la misma banda de frecuencias

Cada década marca unos nuevos hábitos sociales, introduce nuevas pautas de conducta, en definitiva, un estilo de vida que genera sus propias imágenes.

Cuando hace más de diez años se empezaron a usar los teléfonos móviles de coche, nadie podía imaginar el "boom" que iban a tener en España. Pero mientras los españoles tenían la posibilidad de resolver asuntos de negocios o personales desde el coche, en Europa, los altos ejecutivos de la City londinense disfrutaban del último avance tecnológico: el teléfono portátil.

El sistema de comunicación por radio celular inaugura definitivamente una nueva etapa en el mundo de las telecomunicaciones. Su máximo exponente es el teléfono portátil, el único teléfono que nos permite telefonear y ser telefoneados donde deseemos. Su tamaño reducido, como la palma de una mano, permite llevarlo en el bolsillo de la chaqueta junto a las llaves o el mechero.

Cualquier lugar es válido para sacar un teléfono del bolsillo, marcar un número y ponerse en contacto con otra persona. La escena que hoy se ve en las calles de Nueva York, Hong Kong o Londres de un joven encorbatado hablando por teléfono mientras cruza andando un semáforo constituye una nueva forma de comunicación que ya es posible en España.

Recientemente han comenzado a comercializarse en nuestro país los primeros modelos de estas características, la comunicación se establece mediante un sistema celular cuyo funcionamiento está basado en la emisión de señales celulares que conectan con la red de Telefónica.

En España, la aparición del teléfono portátil se debe a la puesta en marcha por parte de Telefónica del nuevo servicio de telefonía móvil TMA 900. Hasta ese momento, las comunicaciones móviles en nuestro país se servían de la banda de frecuencia de 450 Megaherzios, un servicio que actualmente ya se encuentra saturado en Madrid.

La fiebre que se ha extendido como la pólvora de hablar por teléfono desde el coche, ayudada por el descenso del precio de los aparatos, ha creado un mercado en ebullición. Con la aparición del teléfono portátil este hábito se verá incrementado, pues no solamente el recibir y efectuar llamadas se circunscribirá al espacio interior de un coche. Se estima que para finales de 1991 habrá en España en torno a 120.000 abonados a la telefonía móvil, aunque en el año 2000 los clientes potenciales sobrepasarán los tres millones de personas sólo en España.

**ENTORNO DINÁMICO**

Mientras tanto la moda de hablar por teléfono desde la calle, tiene su razón de ser. La dura competencia que impone un entorno cada vez más dinámico refleja inequívocamente nuevas necesidades de comunicación. Solucionar una urgencia, obtener una información valiosa al instante, se encuentre uno donde se encuentre, no es ya sólo exclusivo de jóvenes encorbatados. La toma de decisiones en la que se apoya el progreso de la sociedad afecta a todas las esferas de la vida social.

En consecuencia, un nuevo mercado de las telecomunicaciones ha quedado inaugurado en España y los fabricantes de estos equipos se han lanzado a la comercialización de los primeros teléfonos portátiles que funcionan en la frecuencia de banda de los 900 megaherzios, frecuencia en la que Telefónica ha invertido 17.500 millones de pesetas.

Actualmente se pueden efectuar llamadas desde la provincia de Madrid, Palma de Mallorca y pronto también desde Valencia, Barcelona, País Vasco, Sevilla, Málaga, Alicante y Cádiz.

Pero esto es sólo el principio. A partir de 1993 será introducido en España el servicio de Telefonía Móvil Digital paneuropeo (GSM) impulsado por la Comunidad Europea y en el que también NEC multinacional de las comunicaciones y la informática está participando activamente. Este servicio ofrecerá a todos los usuarios del territorio comunitario la misma banda de frecuencia. Con esta iniciativa se pretende acabar con las incompatibilidades entre las redes celulares de los distintos países de la CE.

Acercarse por encima de las distancias, de las ideologías o el tiempo es ya una realidad. Con el nuevo concepto de las comunidades telefónicas todos nosotros podremos ser fácilmente localizados por pequeños aparatos cada día más ligeros y cómodos de llevar.

Teléfono celular portátil

Fabricación de sistemas de conmutación digital

**5. NOTICIA DEL DESPLIEGUE DE LA RED GSM EN ESPAÑA [6]**

El servicio de voz ha sido el principal elemento para impulsar este mercado, convertido en un mercado de masas con un índice de penetración del 98.7% de la población mundial. Además, GSM tiene más capacidades aparte de la voz, dividiéndose sus servicios en dos grupos:

- Servicios básicos.
    - Servicios portadores. La red únicamente presta servicios de transmisión de datos, sin entrar en el contenido. Estos servicios son datos por conmutación de circuitos a 300, 1200, 2400, 4800 y 9600 bps.
    - Teleservicios. Son aquellos servicios que proporcionan plena capacidad de comunicación entre usuarios. Los servicios soportados por GSM son telefonía (voz), llamadas de emergencia, servicio de mensajes cortos (SMS) y fax automático de grupo III.
- Servicios suplementarios. Servicios adicionales como por ejemplo autentificación de usuarios, identificación de llamada entrante, restricción de llamadas, transferencia de llamadas, llamada en espera, multiconferencia y grupo cerrado de usuarios.

Limitaciones del sistema GSM para la transmisión de datos:

- El sistema GSM es un estándar orientado a circuitos, por lo que la conexión asigna un recurso radio en exclusiva para el cliente y se tarifica por tiempo.
- Hay poco mercado de aplicaciones estándares de transmisión de datos, todo son soluciones propietarias elevando el precio de éstas.

Esto hace de GSM que no sea adecuado para el acceso a Internet ya que la forma más adecuada es la conmutación de paquetes ya que la información se genera a ráfagas. Por ello, se definió GPRS orientado a paquetes, por lo tanto más adecuada para la transmisión de datos.

Las características de GPRS son las siguientes:

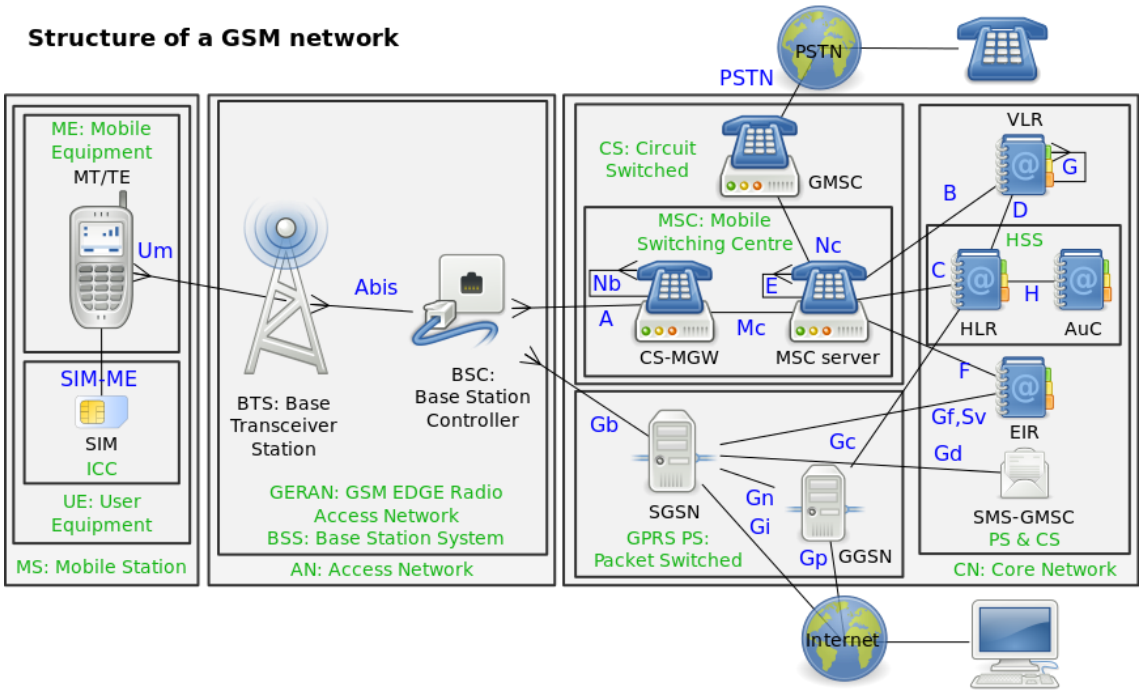
- Eficiencia espectral, dando recursos en el enlace de subida y bajada de forma separada, adecuándose a la asimetría de la mayoría de servicios.
- Bajo coste de implantación reutilizando el hardware diseñado para GSM.
- Mejores prestaciones de velocidad, ya que cada *slot* temporal permite hasta 21.4 Kbps
- Calidad de servicio de forma que pueda soportar diferentes clases de servicio con diferentes prioridades.

Los siguientes puntos del capítulo se dedicarán a exponer la arquitectura y funcionamiento del estándar GSM. El estándar completo son miles de páginas, por lo que esto será sólo un resumen de sus características más destacables.

## 2.2 ARQUITECTURA

El sistema GSM se compone de cuatro bloques que son:

- La estación móvil (MS)
- El subsistema de estación base (BSS)
- El subsistema de conmutación y de red (CN)
- El subsistema de operación y mantenimiento (MNS)



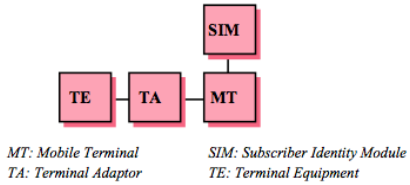

**6. ARQUITECTURA RED GSM+GPRS [7]**

A continuación se detallará la funcionalidad de cada uno de los bloques.

### 2.2.1 LA ESTACIÓN MÓVIL, MS:

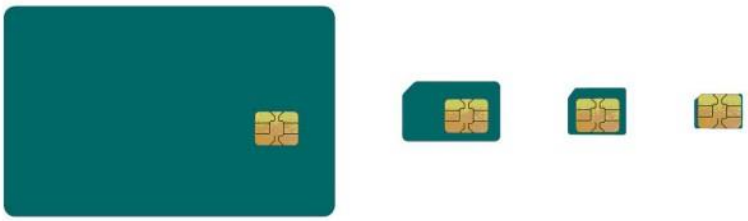
**7. PRIMEROS MÓVILES GSM DE TELEFÓNICA [6]**

El equipo móvil permite al usuario acceder a los servicios que ofrece el operador móvil. Dicho término está asociado a diferentes elementos, siendo los más importantes el equipo móvil y la tarjeta SIM. Esto permite desasociar el teléfono móvil del abonado.




**8. ARQUITECTURA DEL EQUIPO DEL ABONADO [3]**

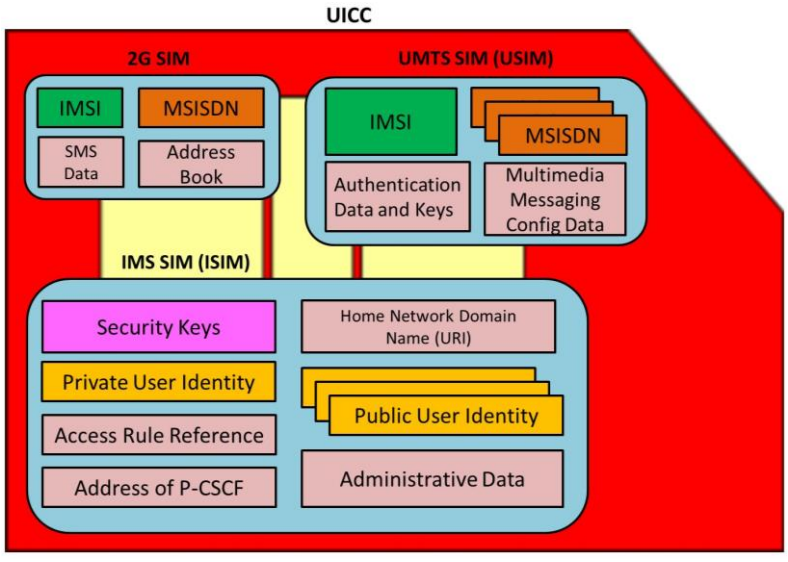
La tarjeta SIM es una tarjeta inteligente de diferentes tamaños en función del equipo móvil en el que vaya a funcionar.



**9.TAMAÑOS DE SIM. ESTÁNDAR, MINI, MICRO Y NANO [8]**

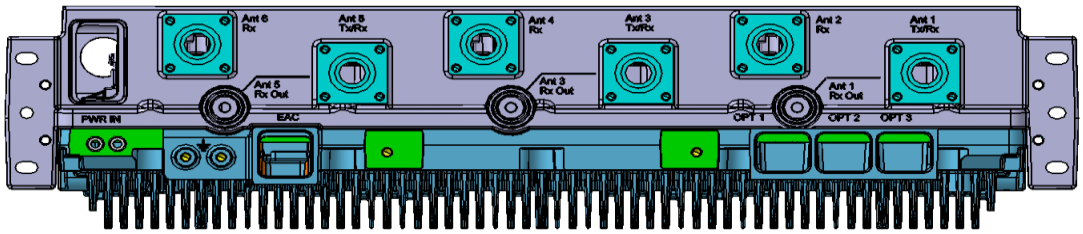
Ésta contiene la siguiente información:

- PIN. Código de 4 cifras para acceso a la información de la SIM.
- PUK. Código de 8 cifras para el desbloqueo de la tarjeta.
- Ki. Clave de autenticación en la red GSM.
- Algoritmos usados para la autenticación del abonado (A3) y para generar la clave de encriptación (A8).
- IMSI. Identificador del subscriptor, es usado por la compañía para mantener un registro de la actividad del abonado y realizar la facturación. Número de entre 14 y 15 cifras, único. Almacenado también en los subsistemas AuC, HLR y VLR que se verán más adelante. Compuesto por varios campos:
    - MCC. Código del país. 3 cifras.
    - MNC. Código del operador de telefonía. 3 cifras.
    - MSIN. Identificador del subscritor. 9 cifras.




**10. ARQUITECTURA SIM 2G/3G [9]**

### 2.2.2 SUBSISTEMA DE ESTACIÓN BASE BSS:




**11. FLEXI BTS DE NOKIA CON 3 SECTORES [10]**

Es el encargado de controlar la interfaz radio, permitiendo la comunicación entre el MS y la red de comunicaciones. Este subsistema está compuesto por dos partes:

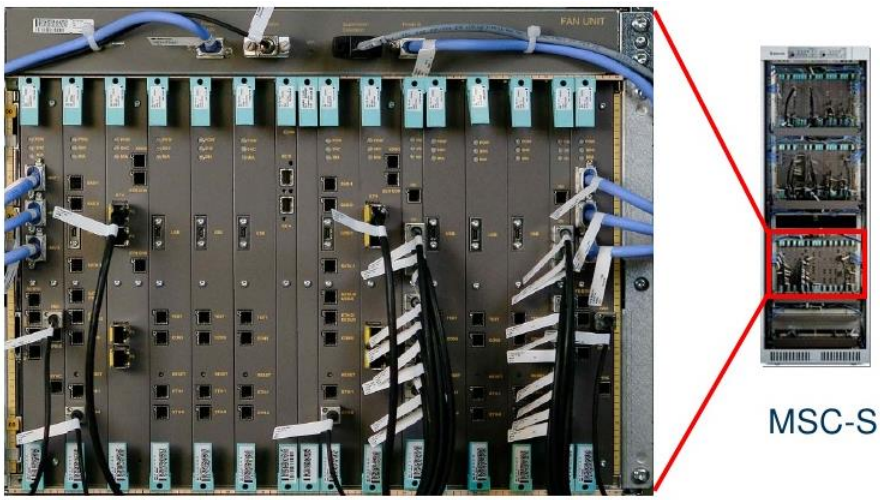
- Transceptor de Estación Base o BTS. Es el punto de comunicación radio entre el MS y el resto de la red. Transmite y recibe las señales, realiza la modulación, control de potencia, multiplexado, codificación/decodificación y cifrado de las señales. Normalmente se ubica en el centro geográfico de la celda.
- Controlador de Estación Base o BSC. Es la "inteligencia" de la BSS, controla varias BTSs y gestiona las operaciones de traspaso, canales radio y otras funciones de control.
- Unidad TRAU. Es la encargada de la adaptación entre la tasa de transmisión del MS a 16kbps y la tasa de la señal de voz de la red de conmutación convencional a 64kbps. Este elemento se puede ubicar indistintamente en la BTS, BSC o MSC.

### 2.2.3 SUBSISTEMA DE RED Y CONMUTACIÓN, NSS:

El principal objetivo del NSS es configurar la red para permitir la comunicación entre dos usuarios. Para ello es capaz de controlar múltiples BSS y realiza la conmutación y encaminamiento de llamadas dentro de la red del operador así como la conexión a otras redes públicas. Dispone de los siguientes elementos:

- Centro de conmutación móvil, MSC. Es el núcleo de toda NSS. Controla diferentes BSCs y es el responsable del encaminamiento de las llamadas. Gestiona también los procesos de registro, autenticación, información de localización y traspaso de llamadas.
- Registro local, HLR. Es una base datos de los abonados en la que se almacenan datos de cada usuario como:
    - Número de teléfono.
    - Localización actual del abonado.
    - Servicios permitidos.
    - IMSI.
    - Ki.
- Registro de visitantes, VLR. Es una base de datos cuyo objetivo es evitar que todas las peticiones se realicen al HLR. Se almacena la información de los abonados que son de otra red e información temporal de los abonados propios de una zona geográfica concreta.
- Pasarela móvil GMSC. Es el elemento de interconexión entre la red pública PSTN y la red GSM del operador. Este equipo es el encargado de realizar las peticiones de llamadas desde la red pública a la red GSM, ya que la red pública es incapaz de realizar peticiones al sistema HLR directamente.
- Puerta de enlace del servicio de mensajería, SMS-G. Es el equipo encargado de gestionar el servicio de mensajes cortos, SMS. Su forma de operar es almacenando el mensaje y reenviando cuando el terminal de destino esté operativo.

- Centro de autenticación, AuC. Este sistema mantiene una base datos con la identificación y la información de autenticación necesaria para cada abonado. Genera 3 datos: un número aleatorio(RAND), una respuesta firmada(SRES) y la clave de la sesión (Kc.) Dispone de datos como:
    - IMSI.
    - Identificador de Área, LAI.
    - Ki.
- Registro del equipamiento, EIR. Dispone de tres listas:
    - Blanca. Equipo permitido.
    - Negra. Equipo bloqueado.
    - Gris. Equipo sin el acceso denegado pero sí se le lleva un seguimiento.




**12. EJEMPLO DE CONMUTADOR GSM DE ERICSON**

### 2.2.4 SUBSISTEMA DE OPERACIÓN Y MANTENIMIENTO, OSS:

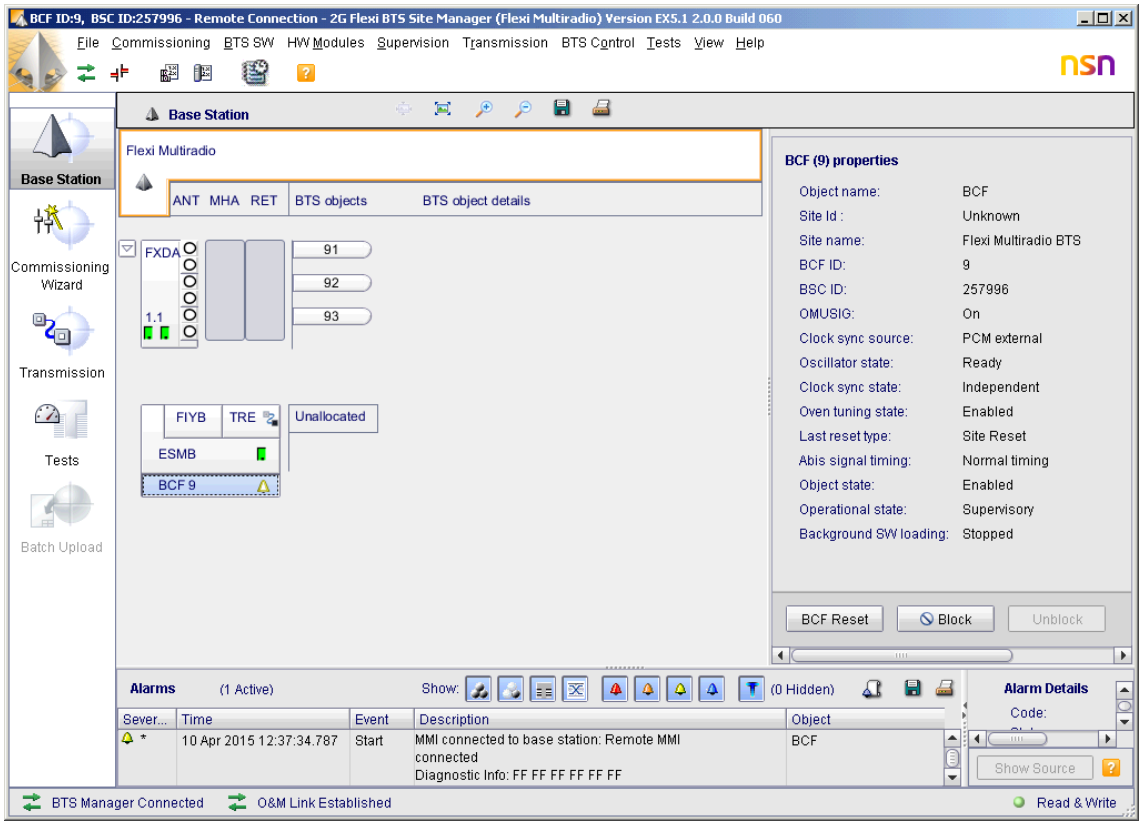
Este subsistema de GSM se encarga de las acciones necesarias para conseguir un buen funcionamiento de la red en cuestión. Entre dichas acciones se encuentran las de solucionar problemas y fallos que puedan aparecer, o monitorizar y mejorar la configuración de los equipos para aumentar su rendimiento.

Existen tres dominios de actuación según el equipo considerado:

- Mediador operador-equipo: Control de los equipos que controlan el tráfico.
- Control de la subscripción: Gestión de abonados y tarificación.
- Operación y mantenimiento: Gestión de los equipos de la red.

Todo se centraliza en el Network Management Center, cuyas funciones más relevantes son:

- Operación integrada de toda la red.
- Monitorizar alarmas.
- Presentar el estado de las redes regionales.
- Gestionar el tráfico de la red.
- Puede tomar responsabilidades regionales.
- Ayudar a la planificación de la red.




**13. EJEMPLO INTERFAZ DE CONFIGURACIÓN DE UNA BTS NOKIA**

## 2.3 INTERFACES DEL SISTEMA GSM

En este punto se van a describir cómo se conectan entre sí los subsistemas descritos en el apartado anterior. Entre cada par de elementos de la red GSM se especifica una interfaz definida por un protocolo de comunicaciones concreto y unos mensajes de comunicaciones. Los protocolos y mensajes que se intercambian los diferentes subsistemas se pueden dividir en dos categorías: tráfico y señalización. Los protocolos y mensajes de tráfico son los que transportan la información del abonado hasta el MSC. Los protocolos y mensajes de señalización se encargan de dar soporte al resto de subsistemas.

En este caso nos centraremos en la interfaz radio, ya que es la parte más importante para nuestro proyecto. Se hará una descripción en capas o niveles, desde el nivel más bajo, la parte física de la transmisión por ondas, hasta el nivel superior de la jerarquía encargado de transmitir la voz del abonado. Como se ha comentado al principio, las interfaces desde radio hasta la MSC, transportan el tráfico del abonado junto con la señalización del mismo. Se estudiará también en este punto la señalización necesaria para poder crear un canal de comunicaciones entre al abonado y la MSC.

Puesto que todo está interrelacionado, para hacer más sencilla la comprensión del sistema se va a estudiar primero cómo el MS y la BTS se comunican por radio, es decir un canal físico de comunicaciones, y después subiremos un nivel de abstracción para poder estudiar los diferentes tipos de canales lógicos que se pueden crear haciendo uso de ese canal físico. Finalizaremos el capítulo comentando cómo utilizar los canales lógicos para poder transmitir la señalización y tráfico del abonado para cursar una llamada o enviar un SMS.

### 2.3.1 CAPA FÍSICA DEL ENLACE RADIO

En este apartado se va a exponer de forma resumida cómo se procesa una señal desde el móvil o BTS para adecuarlo a las características de un entorno de comunicaciones móviles. Comenzaremos

por cómo transformar un flujo de bits en una señal analógica preparada para ser enviada a los amplificadores y/o antenas. Después estudiaremos cómo los mensajes que genera el sistema se modifican para poder minimizar los errores presentes en la comunicación móvil. Terminaremos con el estudio de los canales físicos en los que MS y BTS pueden montar diferentes canales lógicos y una técnica llamada salto en frecuencia.

### MODULACIÓN GMSK

La modulación utilizada en GSM se llama GMSK de sus siglas en inglés *Gaussian Minimun Shift Keying*. Es un caso particular de modulación MSK muy eficiente espectralmente. Con la finalidad de atenuar los lóbulos laterales que genera MSK, se efectúa un procesamiento previo en banda base. En concreto, se hace pasar la señal por un filtro gaussiano de ancho de banda *B*, suavizándose así las transiciones de 0 a 1 y viceversa.

El esquema para la generación de la señal es el siguiente:

**14. DIAGRAMA DEL MODULADOR GMSK**

A la señal binaria de información se le aplica un codificador diferencial que combina los bits $d_i$ y $d_{i-1}$, obteniendo su suma módulo 2:

$$d_k = d_i \oplus d_{i-1}$$

El impulso modulador se define como:

$$\alpha_k = 1 - 2d_k$$

El impulso modulador básico $g(t)$ es:

$$g_k(t) = \alpha_k rect_T(t) h(t)$$

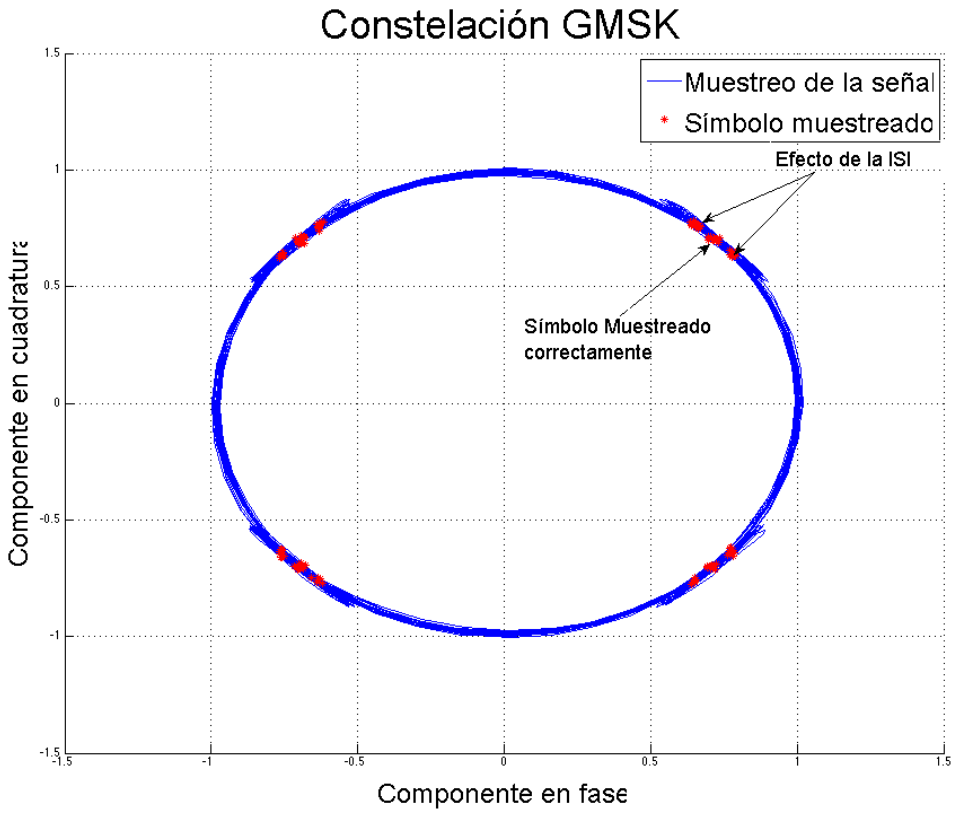
Donde $h(t)$ es el filtro gaussiano que tiene de expresión:

$$h(t) = \frac{1}{\sqrt{2\pi}\sigma \mathrm{T}} exp\left[-\frac{t^2}{2\sigma^2 T^2}\right]$$

La clave de este filtro está en la selección de $BT$ definido en el parámetro $\sigma$:

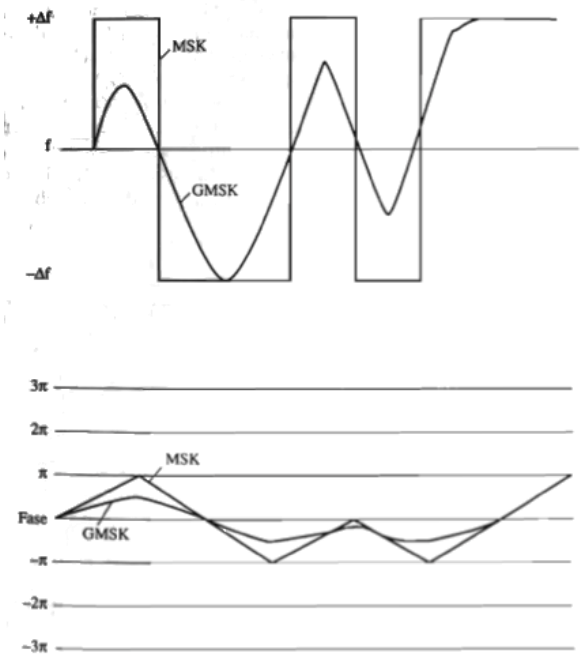
$$\sigma = \sqrt{\ln 2}\ /2\pi BT$$

El filtro gaussiano usado en GSM tiene una característica $BT$=0.3. Este filtro es el encargado de mejorar la eficiencia en ancho de banda y junto al impulso modulador se tener una envolvente constante, por lo que es insensible a las no linealidades presentes en los amplificadores de potencia.




**15. CONSTELACION GMSK DE GSM**

La constelación de este esquema de modulación presenta cuatro estados posibles, como se puede ver en el gráfico 15. Constelacion GMSK de GSM, pero realmente se transmite 1 bit/símbolo, en el que cada símbolo corresponde a una transición de $+\text{-}\pi/2$ rad. En la siguiente gráfica se puede observar con más claridad las transiciones entre símbolos, junto con una comparativa con MSK.



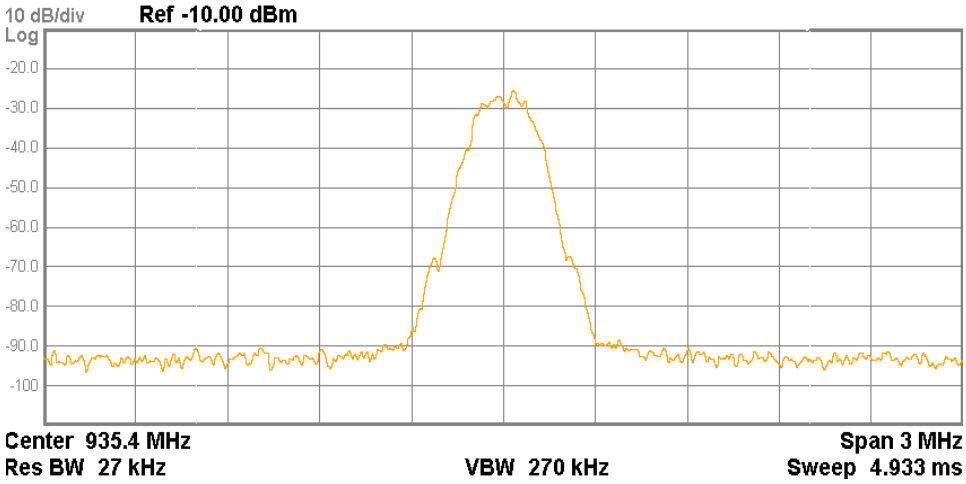

**16. COMPARACIÓN DE VARIACIÓN DE FRECUENCIA Y FASE EN MSK Y GMSK**

La fase de la onda moduladora es:

$$\varphi(t) = \sum_{k} \pi m \int_{-\infty}^{t-kT} g_k(u)du$$

Donde $m$ es el índice de modulación, que en este caso es ½. Por lo tanto, la máxima excursión de la fase es $\pm\pi/2$ rad como se puede observar en la gráfica 16. Comparación de variación de frecuencia y fase en MSK y GMSK.

Esta modulación presenta el problema de interferencia entre símbolos debida a la reducción del espectro, pero es pequeña y se compensa con el uso de ecualizadores de canal.

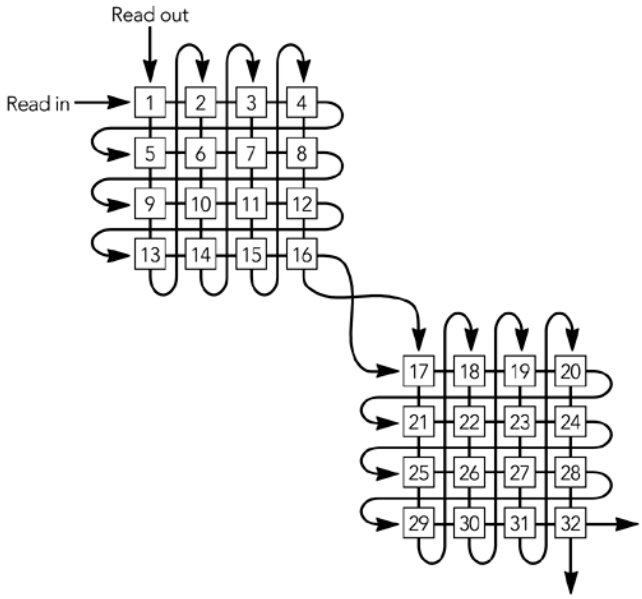



**17. ESPECTRO GMSK DE UNA SEÑAL GSM**

En la anterior figura 17. Espectro GMSK de una señal GSM, tomada en el laboratorio, se observa el espectro de una señal GMSK. Ese espectro es constante en el ancho de banda. También se pueden observar los dos lóbulos laterales pequeños que introduce el filtrado gaussiano previo de dicha modulación. Gracias a esto se consigue un rendimiento espectral aproximado de 1 bit/s/Hz.

### ENTRELAZADO

El entrelazado pretende evitar que los errores que se producen en el canal estén todos agrupados en ráfagas o bloques de bits continuos. Para evitar esto, se intenta conseguir que los errores estén dispersos de forma aleatoria a la entrada del decodificador de los bits. La forma de conseguirlo es enviando los bits sobre el canal en un orden diferente a cómo se han generado. De esta forma, los posibles errores no ocupan posiciones consecutivas una vez desentrelazados en el receptor. Una forma sencilla de hacerlo es guardando el flujo de bits en una matriz por filas y extraerlos, para su modulación, por columnas como muestra el siguiente diagrama:




**18. EJEMPLO DE ENTRELAZADO POR MATRIZ**

En este diagrama si aparece un error en los bits 1, 2 y 3 por ejemplo, al decodificar, estarán separados 4 bits de distancia entre ellos.

### CODIFICACIÓN DEL CANAL

La codificación del canal trata de disminuir los errores en la interpretación de la señal recibida, ya que en un entorno móvil es muy difícil mantener los parámetros de calidad por encima de un umbral. Debido al carácter móvil, se producen fluctuaciones en el nivel de potencia recibida, por lo que se codifica la información añadiendo redundancia para permitir detectar y corregir los errores producidos por el canal de comunicaciones.

Se define la ganancia del código como la reducción en la relación señal-ruido necesaria para obtener una determinada probabilidad de error de bit en un canal con ruido blanco gaussiano.

Para el caso de GSM, el audio se genera a una tasa de 260 bits cada 20ms, es decir, a 13kbps. El codificador empleado, RPE-LTP *(Regular Pulse Exciting–Linear Term Predictor)*, genera bits con diferente importancia debido a la calidad subjetiva del audio, es decir, hay componentes más relevantes que otros en todo el audio. Por lo tanto, se clasifican esas componentes en tres clases de importancia decreciente, medida como la calidad subjetiva en función de la probabilidad de error. Las clases son:

- Ia: Primera clase, 50 bits+3 bits paridad+4 bits relleno + código convolucional de tasa ½ = 114 bits.
- Ib: Segunda clase, formada por los 132 bits siguientes + código convolucional de tasa ½ = 264 bits.
- Ic: Tercera clase, los últimos 78 bits. Sin protección de errores.

La primera clase y segunda, se pasan por un código convolucional de tasa ½ y longitud de influencia $m$=5, lo que produce una secuencia de 378 bits. La última clase no se codifica sino que se transmite tal cual para así ahorrar en ancho de banda, ya que su importancia en la calidad subjetiva del audio no es tan importante como las primeras clases. En total, al final del proceso de codificación de la fuente y canal, se tiene un flujo de 456 bits cada 20ms, 22.8kbps transmitidos en 4 *slot*s temporales, es decir 114 bits por *slot*.

La siguiente tabla muestra un resumen de la codificación y entrelazado de los diferentes flujos de datos, ya sean tráfico de audio o señalización.

| Canal lógico | Tasa de entrada (Kbps) | Bloque de entrada | Codificación de canal | Bloque de salida | Entrelazado |
|---|---|---|---|---|---|
| Tráfico. Máxima velocidad. 9.6kbps TCH/F | 11.2 | 224 | 4 bits relleno + convolucional ½ | 456 | 22 porciones de *slots* desiguales |
| Tráfico. Máxima velocidad. 4.8kbps TCH/F | 6 | 120 | 32 bits relleno + convolucional 1/3 | 456 | 22 porciones de *slots* desiguales |
| Tráfico. Máxima velocidad. 2.4kbps TCH/F | 3.6 | 72 | 4 bits relleno + convolucional 1/6 | 456 | En 8 *slot* mitad |
| Tráfico. Media velocidad. 2.4kbps TCH/H | 3.6 | 144 | 8 bits relleno + convolucional 1/3 | 456 | 22 porciones de *slots* desiguales |
| Canal de sincronización SCH | | 25 | 10 bits paridad + 4 bits relleno + convolucional ½ | 78 | |
| Canal de acceso aleatorio RACH | | 8 | 6 bits paridad + 4 bits relleno + convolucional ½ | 36 | |
| Otros canales. FACCH, TCH/8, SACCH, BCCH, PAGCH. | | 184 | Código FIRE 184/224 + convolucional ½ | 456 | En 8 *slot* mitad o 4 *slot* completos |

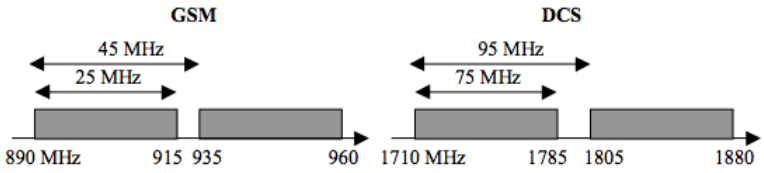
**19. TABLA DE CODIFICACION CANALES EN GSM**

### CANALES FÍSICOS

El estándar GSM, en el documento TS 45.005 describe que es un sistema FDD/FDMA/TDMA, e incluye todas las combinaciones de bandas de frecuencias permitidas por el estándar:

- FDD: Diferentes bandas de frecuencia para los enlaces descendente y ascendente, lo que permite una comunicación full dúplex.
- FDMA: Cada banda de frecuencias, ascendente y descendente, está dividida en canales, cada uno de ellos con una frecuencia diferente.
- TDMA: Cada canal está a su vez dividido en *slots* temporales.

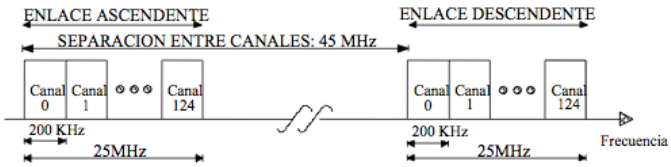
Para la parte FDD, el sistema GSM900 usa la banda de frecuencias de 890 hasta 915Mhz para el enlace ascendente y la banda 935 a 960Mhz para el enlace descendente. En el sistema DCS1800, el enlace ascendente está entre 1710 y 1785Mhz y el descendente entre 1805 y 1880Mhz.




**20. ESPECTRO USADO POR GSM**

Para FDMA, los 25Mhz de ancho de banda del sistema GSM900 para cada sentido de la comunicación se subdividen en 124 canales de 200Khz de ancho de banda cada uno. Los dos canales de los extremos no se utilizan porque cada uno de los 124 canales ocupa en la práctica 270Khz por el tipo de modulación empleada.

Esta división es similar para el sistema DCS1800, sólo que en este caso el ancho de banda de cada sentido es de 75Mhz por lo que se dispone de 372 canales. En total ambas bandas cuentan con 494 canales.




**21. CANALIZACIÓN DE LA BANDA GSM900**

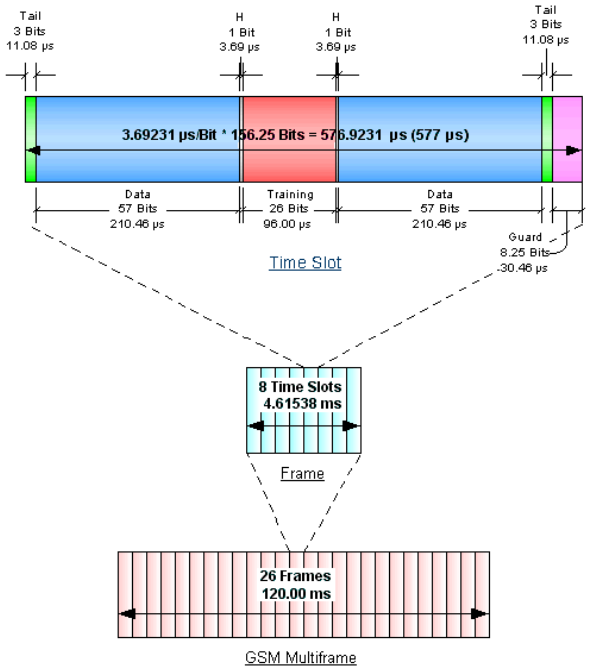
Cada canal, tanto en GSM900 como en DCS1800 se identifica por su ARFCN (*Absolute Radio Frecuency Channel Number*). La correspondencia entre el ARFCN y la frecuencia se puede calcular de la siguiente forma para GSM900:

$$1 \leq n \leq 124 \begin{cases} F_{uplink}(n) = 890 + 0.2n \\ F_{downlink}(n) = F_{uplink}(n) + 45 \end{cases}$$

Y para el caso de DCS1800, la frecuencia del canal se obtiene como:

$$512 \leq n \leq 885 \begin{cases} F_{uplink}(n) = 1710.2 + 0.2(n - 512) \\ F_{downlink}(n) = F_{uplink}(n) + 95 \end{cases}$$

Para terminar, el acceso TDMA subdivide cada frecuencia a su vez en 8 *slots* temporales, obteniendo en total 3952 canales físicos entre las bandas GSM900 y DCS1800.




**22. DIVISION TEMPORAL DE CADA CANAL GSM [11]**

### SALTO EN FRECUENCIA

Esta técnica consiste en transmitir segmentos temporales de la señal en diferentes portadoras de forma pseudoaleatoria. Esta técnica mejora la seguridad de las comunicaciones, ya que un usuario no autorizado no puede decodificar la señal al no disponer de la secuencia de saltos en frecuencia. También permite que posibles desvanecimientos o interferencias no tengan una duración mayor al

segmento temporal que se envía. Una tercera ventaja es que los dispositivos móviles pueden compartir una banda de frecuencia con una interferencia mínima, ya que es poco probable la colisión de diferentes transmisiones haciendo uso de esta técnica y, si se producen, se pueden detectar los errores.

### 2.3.2 Capa enlace de la interfaz Um

En el apartado anterior se ha visto como toda la banda GSM-900 y DCS-1800 se subdivide hasta obtener 3952 canales de transmisión. El siguiente paso en nivel de abstracción es ver qué uso se les dará a todos esos canales y como estructurarlos para un uso eficiente de toda la banda.

#### Canales lógicos

Todos los canales radio se subdividen en dos tipos, canales para cursar tráfico (voz y señalización de usuario principalmente) y canales de control de la red GSM. Nótese que, como se ha visto, el sistema GSM está duplexado en frecuencia por lo que cada canal ascendente tiene un canal simétrico en el enlace descendente.

Vamos a estudiar por separado los canales de control y los de tráfico:

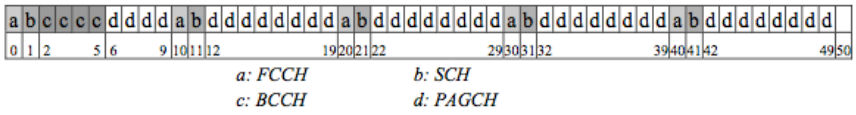
#### Canales de control común:

Los canales de control siempre se disponen en el *slot* temporal 0 de una de las frecuencias asignadas a la BTS.

Los canales de control son los siguientes:

- **FCCH**: *Frecuency Correction Channel*. Se emite la señal portadora piloto de forma que los terminales móviles se puedan sincronizar en frecuencia.
- **SCH**. *Synchronization Channel*. En este canal los móviles sincronizan sus contadores de tramas para conocer las secuencias temporales de los canales BCCH y AGCH/PCH. También se emite el identificador de la estación base, BSIC, y la secuencia de ecualización del canal.
- **BCCH**. *Broadcast Control Channel*. Envía la información necesaria para que una estación móvil pueda acceder a la BTS, incluyendo información de identificación de celda, área, celdas vecinas, etcétera.
- **PCH**. *Paging Channel*. En el canal de *paging* se envían los mensajes de búsqueda de móviles para conocer en qué celda se encuentran.
- **AGCH.** El canal de *Access Grant Channel* se utiliza para responder a una petición de acceso realizada por el móvil con anterioridad. Le indica al terminal el canal de señalización que deberá usar.
- **RACH**. *Random Access Channel*. Canal de acceso utilizado por los terminales móviles para la petición de un canal dedicado.

El diagrama siguiente muestra la distribución temporal de los canales de control dentro de una multitrama de 51 tramas de duración, enviados siempre desde el primer *timeslot* (TS0).



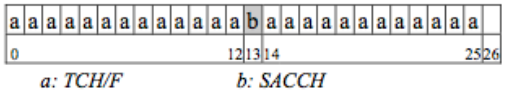

**23. DISTRIBUCIÓN EN MULTITRAMA DE LOS DIFERENTES CANALES DE CONTROL**

#### Canales de tráfico:

Los canales de tráfico son los utilizados por el usuario para la transmisión de señalización y voz de usuario. Hay diferentes tipos de canales:

- **TCH/F**. *Traffic Channel Full Rate*. Canal bidireccional utilizado para la transmisión de información del usuario. Ocupa un *slot* temporal por cada trama.
- **TCH/H**. *Traffic Channel Half Rate*. Igual que el anterior pero a mitad de velocidad, ya que se ocupa un *slot* temporal cada dos tramas.

El diagrama siguiente muestra la agrupación de 26 canales de tráfico. Cada 13 TCHs se enviaría el canal asociado (SACCH) a la comunicación.




**24. DISTRIBUCIÓN DE CANALES DE TRÁFICO**

### CANALES DE CONTROL ASOCIADO:

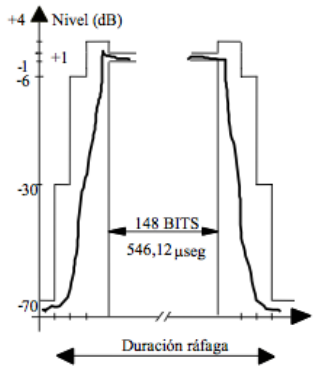
Son canales de señalización entre BTS y MS que están asociados a un canal de tráfico concreto y por ello se transmiten en el mismo *slot* temporal que dicho canal de tráfico. Sirven para gestionar parámetros concretos de la llamada en curso. Existen los siguientes tipos de canales lógicos:

- **SACCH**. *Slow Associated Control Channel*. Canal de señalización lento, los mensajes se intercalan entre las tramas de tráfico al que están asociadas.
- **FACCH**. *Fast Associated Control Channel*. Similar al anterior, pero para mensajes que no pueden esperar, como por ejemplo un traspaso de llamada.
- **SDCCH**. *Stand Alone Dedicated Control Channel*. Canal de señalización general entre la MS y la BTS en el curso de establecimiento de una llamada y antes de asignar un TCH.

### TIPOS DE RÁFAGAS

En GSM cada trama tiene una duración de 4.615ms y cada *slot* temporal de 577us. La información en los diferentes canales, ya sean de control o de tráfico, se realiza en ráfagas en cada *slot* temporal.

Hay diferentes tipos de ráfagas, pero todas ellas tienen los mismos campos, unos bits de información, una secuencia de entrenamiento para ecualización del canal y unos bits de cola. Entre ráfaga y ráfaga se dejan un tiempo de guarda equivalente a la duración de 8.25bits (30.44us) necesario para que los amplificadores de potencia entren y salgan del punto de trabajo.




**25. MÁSCARA DEL TIEMPO DE GUARDA DE UNA RÁFAGA**

Los tipos de ráfagas son los siguientes:

- **Ráfaga de acceso:** Utilizada en el enlace ascendente en las primeras fases de comunicación. Es la utilizada en el canal RACH.

- **Ráfaga S:** Utilizada en los canales SCH para que el móvil se sincronice con la estación base. Menos bits de información que la normal.
- **Ráfaga F:** Todos los bits a 1, usada por el canal FCCH. Genera una señal sinusoidal pura.
- **Ráfaga normal:** Es una trama de 148 bits, con la siguiente estructura:

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

**26. RÁFAGA NORMAL**

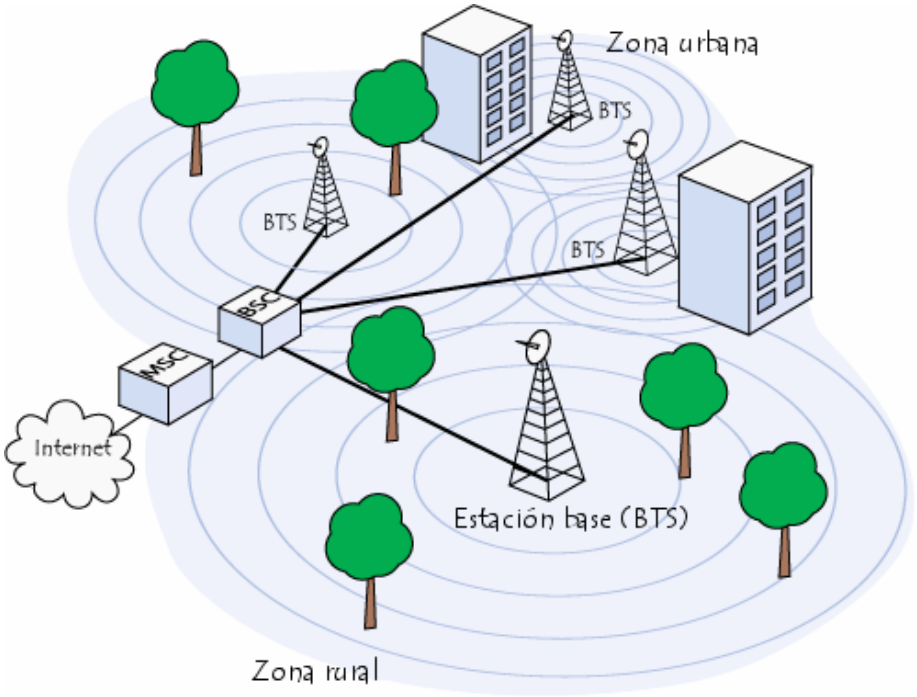
## 2.4 FUNCIONAMIENTO DEL SISTEMA GSM

Hasta ahora se han visto los diferentes elementos que componen el sistema GSM. Ahora se va a mostrar cómo usan esos elementos la red y el terminal móvil para poder proporcionar el servicio de llamadas a los abonados.

Este capítulo se va a dividir en los siguientes apartados:

- Selección de una celda
- Acceso a la red
- Realización de llamadas
- Envío de SMS

### 2.4.1 SELECCIÓN DE UNA CELDA




**27. ILUSTRACIÓN DE UN SISTEMA CELULAR CON 4 CELDAS [12]**

El proceso de selección de una celda será el primer paso para que el abonado obtenga servicios móviles y comenzará cuando el terminal móvil es encendido. Para ello realiza un barrido en la banda GSM para seleccionar aquellos canales de control que recibe con más potencia, con lo que realiza la primera clasificación de frecuencias. Una vez sintonizada la frecuencia guía de una estación, el móvil se sincroniza con el número de trama de FCCH y de esta forma conoce la

ubicación del canal SCH, que contiene los contadores del resto de tramas así como el identificador BSIC. Con esta información se puede obtener la información enviada en el canal BCCH. Gracias a la información de ese canal, el terminal móvil dispondrá de los medios necesarios para poder realizar peticiones de acceso a la red.

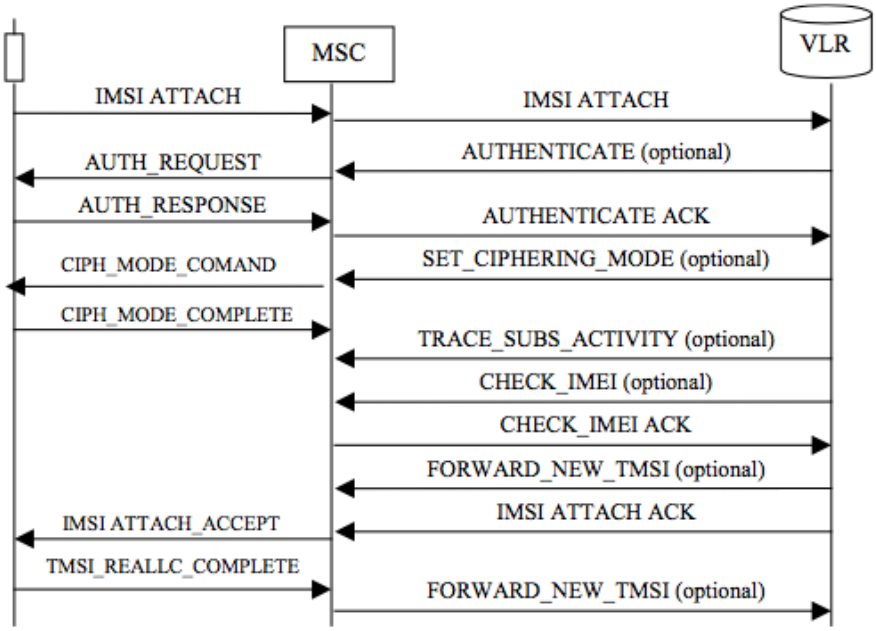
### 2.4.2 ACCESO A LA RED

Este procedimiento consiste en indicarle a la red que el terminal móvil está operativo y puede recibir y realizar llamadas, proceso denominado también como *IMSI attach*.

El móvil comienza con el envío de una ráfaga de acceso por el canal RACH, compuesta por 8 bits. Los tres primeros indican el motivo del acceso (respuesta a un *paging*, llamada de emergencia, restablecimiento de llamada o petición de usuario) y los 5 restantes son un número aleatorio que sirve de identificador temporal de terminal móvil.

Una vez enviado el mensaje, el sistema le asigna un canal de señalización libre, indicándoselo por medio del canal de control y usa el identificador temporal que ha enviado el teléfono previamente.

Una vez dispone de un canal asignado para el acceso a la red, se registra en la MSC a través de un *IMSI attach*, donde el motivo de acceso en la ráfaga RACH es una petición de usuario. Una vez que dispone de recursos para acceder a la red, hace uso de su IMSI para poder obtener permiso a la hora de realizar llamadas y recibirlas. El sistema le asigna un TMSI para que lo utilice como identificador temporal más corto e intentar controlar la confidencialidad de las comunicaciones.




**28. PROCESO DE IMSI ATTACH COMPLETO**

El proceso del diagrama anterior es el proceso completo de *IMSI attach*, ya que incluye los mensajes relativos al cifrado de la comunicación. La parte esencial es la petición de *IMSI attach* por parte del móvil a la MSC y ésta al VLR, así como la respuesta del VLR a la MSC del ACK de dicha petición y la respuesta de la MSC al móvil con la aprobación de la solicitud.

### 2.4.3 REALIZACIÓN DE LLAMADAS

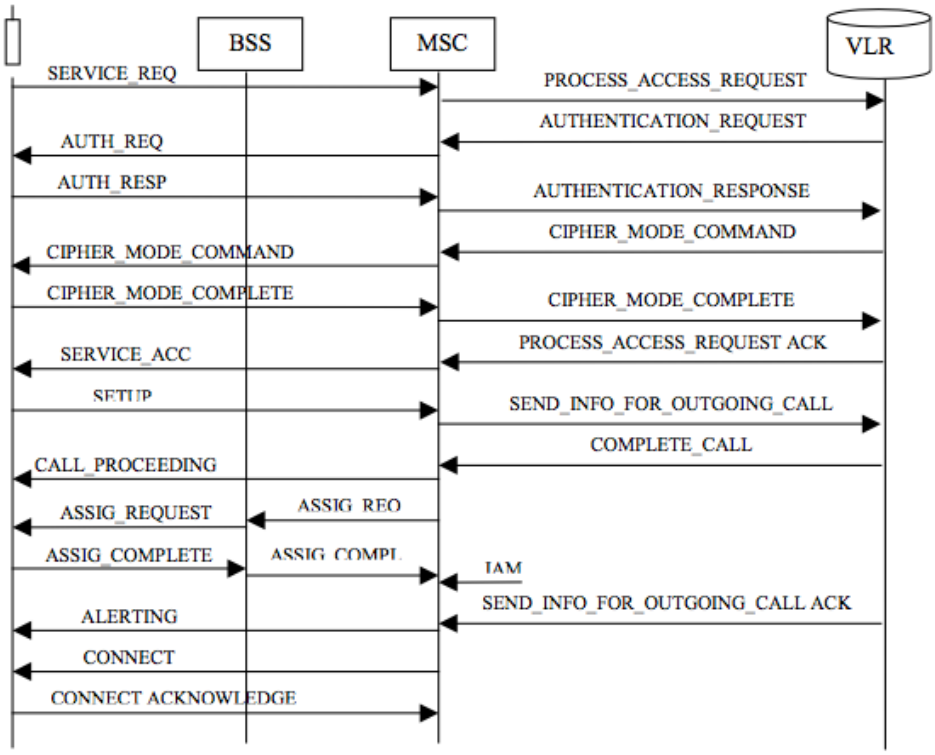
Existen dos procesos diferentes en cuanto a la gestión de llamadas, las llamadas iniciadas desde un terminal móvil y las llamadas dirigidas hacia un terminal móvil.

LLAMADA ORIGINADA EN MÓVIL.

Una vez marcado el número de teléfono y pulsada la tecla descolgar, el móvil inicia un acceso a la red por el que se le asignarán unos recursos radio (básicamente un TS dentro de un canal de la celda que le da cobertura). En este caso, el motivo es una petición de usuario, motivo que se incluye dentro del campo de petición de acceso por el canal RACH.

El establecimiento de llamada tiene dos pasos: creación del canal de comunicaciones entre terminal móvil y MSC y la creación del canal de comunicación entre MSC y el otro extremo de la llamada.

La primera fase corresponde al estándar GSM y permite realizar la gestión de recursos. La segunda parte sigue el estándar ISDN y la señalización por SS7 que no se detallará en este documento.



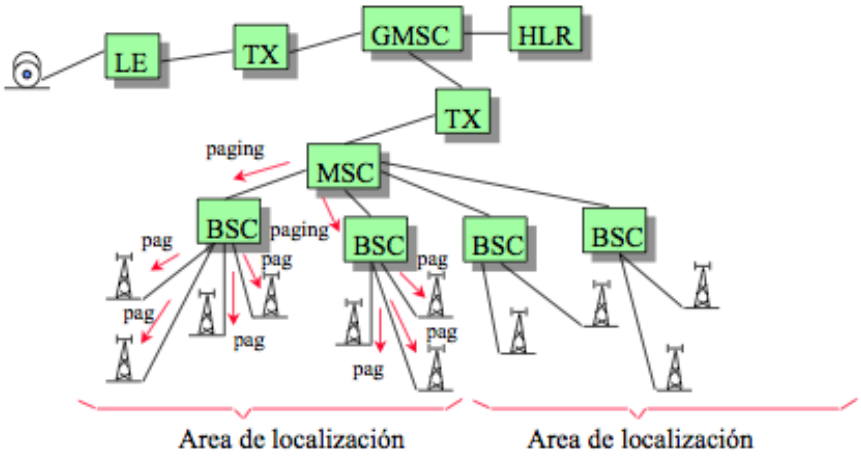

**29. PROCESO DE REALIZACIÓN DE LLAMADA ORIGINADA EN MÓVIL**

El diagrama anterior muestra el proceso completo seguido por móvil, MSC y VLR para realizar una llamada originada en el móvil. Comienza la secuencia realizando el MS una petición al MSC y ésta a su vez al VLR para comprobar si tiene permiso o no el MS para realizar la llamada. Después estaría el proceso de autenticación del MS dentro de la red hasta que consigue el acceso (línea SERVICE_ACC). Tras esto, hace la petición para configurar la red para realizar la llamada y la MSC le indica al VLR dicha configuración. El MSC le asigna los recursos radio necesarios para la BTS y ésta al MS. Una vez todo el camino de la voz está configurado, se realiza la petición IAM *(Initial Address Message)* para la llamada. Tras ese mensaje, se envía el tono al MS origen, y una vez descolgado en el otro extremo, se realiza la conexión.

LLAMADA RECIBIDA EN MÓVIL.

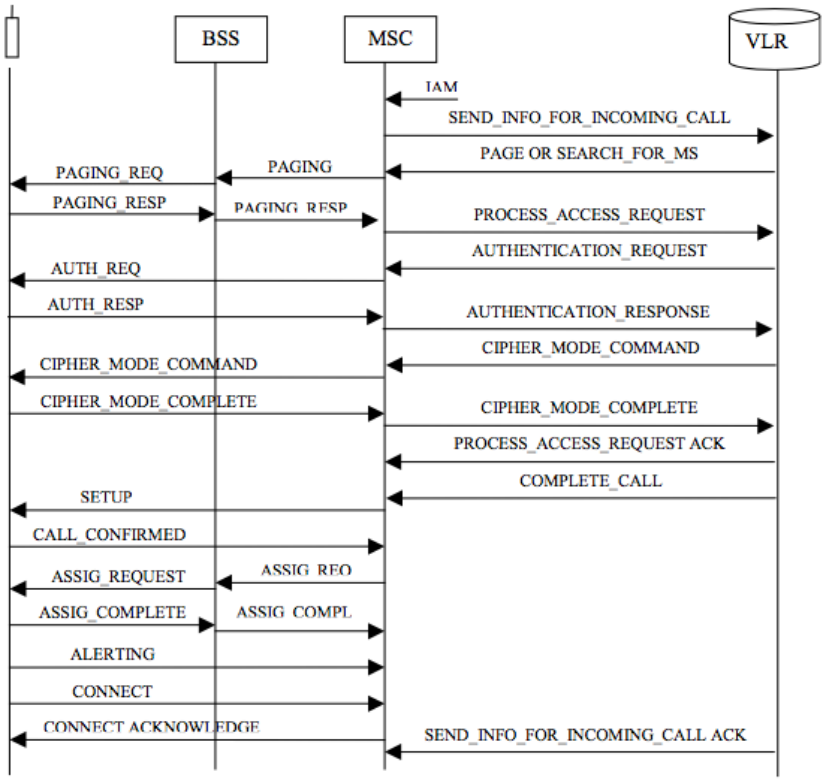
En este caso, cuando un abonado realiza una llamada a un terminal móvil, la numeración distingue al operador GSM de destino, con lo que se encamina la llamada hasta el GMSC del operador. Una vez en el GMSC se consulta al HLR para conocer la localización de dicho terminal. Con esa localización se conoce el MSC de destino, creándose el canal entre las MSC origen y destino. Falta crear el canal entre al MSC destino y el móvil destino, que es lo que se va a detallar en este

apartado. Para ello el MSC realiza una búsqueda de móvil hasta obtener la BSC en la que se encuentra. Envía un mensaje BSSMAP PAGING a todos los BSC dentro del último LAC en el que se encontraba el móvil y éstos a su vez lo reenvían a las BTS por medio del canal PCH para conocer la celda en la que se encuentra el terminal.




**30. EJEMPLO DE ENVÍO DE MENSAJE DE PAGING POR LA ZONA DE COBERTURA DEL MÓVIL**

Una vez conocida, la BSC realiza una reserva de un canal radio para la BTS en la que se encuentre el móvil y envía un mensaje de alerta al terminal para que el abonado descuelgue el móvil.




**31. MENSAJES TRANSMITIDOS PARA ESTABLECER UNA LLAMANDA HACIA UN MÓVIL**

En el anterior diagrama se muestra cómo le llega un mensaje de llamada a la MSC en la que se encuentra el móvil (mensaje IAM). Después, la MSC envía la configuración necesaria de la llamada entrante al VLR, y éste le responde con los datos de PAGING para buscar el MS dentro de la red

como se ha visto en el diagrama 30. Ejemplo de envío de mensaje de paging por la zona de cobertura del móvil. Una vez hay respuesta del MS, se realiza el proceso de autenticación y cifrado de la comunicación. Tras todo ese proceso el VLR emite el mensaje PROCESS_ACESS_REQUEST_ACK e indica a la MSC la configuración para la llamada entrante. El MSC, con esta información, asigna los recursos radio necesarios a la BTS y MS. Una vez el canal radio está configurado para recibir la llamada, se informa al móvil que tiene una llamada entrante para que descuelgue y se pueda realizar dicha comunicación.

### 2.4.4 Envío y recepción de SMS

El estándar TS 23.040 de GSM describe la capacidad de transmisión de mensajes de texto cortos. Éstos están limitados a 160 caracteres, aunque se pueden enviar SMS más largos, dividiéndose en grupos de 160, para lo que el protocolo añade una marca que indica que todos van en un único grupo.

Los mensajes se envían por medio del canal de tráfico o señalización asignado de forma indistinta hasta un centro de mensajes, que los almacena en una cola hasta que el destino esté disponible y se lo hace llegar, de forma independiente si está o no realizando una llamada o transmitiendo datos.

### 2.4.5 Seguridad en GSM

Vamos a dividir la seguridad en la red GSM en tres aspectos diferentes pero complementarios:

- Confidencialidad de la identidad del abonado.
- Autenticación en la red GSM.
- Cifrado de las comunicaciones.

#### Confidencialidad del abonado:

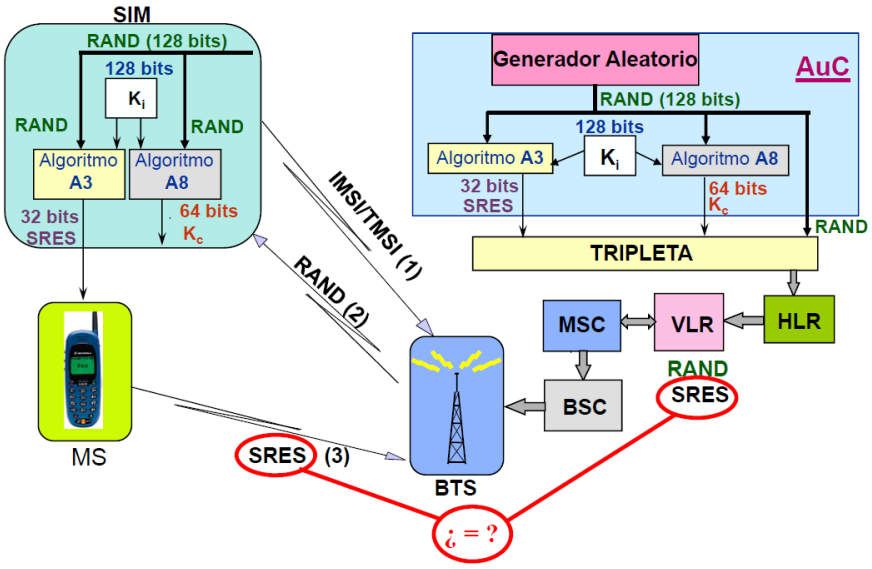
El abonado está identificado, como ya se ha visto con anterioridad, mediante su IMSI. La finalidad de este procedimiento es asegurar que el IMSI no se envía sin cifrar vía radio, de forma que no se pueda interceptar en una comunicación.

La forma de proceder es asignar un identificador temporal parecido al IMSI, llamado TMSI. Dicho TMSI sólo tiene validez dentro de un área de localización, aunque hay casos puntuales en los que el móvil necesita enviar el IMSI sin cifrar, como por ejemplo: al cambiar de VLR y éste no consigue identificar el VLR antiguo; cuando hay un *IMSI attach* al encender el móvil; o cuando el VLR ha borrado los datos del móvil por llevar mucho tiempo sin tener actividad.

#### Autenticación en la red GSM:

Este es el método por el cual la red gestiona los accesos a la misma, de forma que sólo aquellos móviles con credenciales válidas podrán acceder a la misma y utilizar sus servicios. En este caso se utiliza la información de la clave Ki y también el IMSI, almacenados ambos en la SIM del abonado. La clave Ki se encuentra en el servidor AuC de la red. Esta clave no la envía el móvil, sino que es el operador el que, al entregar la SIM al abonado, previamente ha guardado esa clave en el AuC.

El procedimiento para acceder a la red, tras disponer el HLR-VLR del IMSI y TMSI:




**32. PROCEDIMIENTO DE AUTENTICACION EN UNA RED GSM**

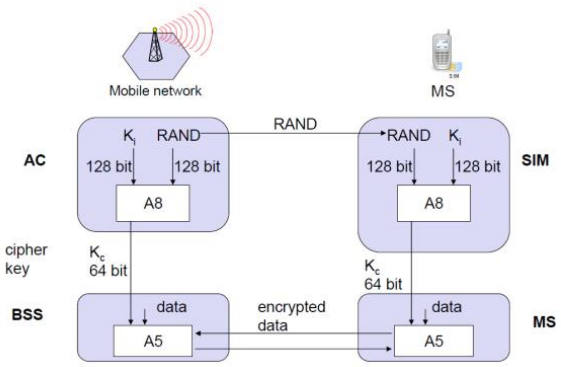
1. El AuC, usa un número aleatorio RAND de 128 bits, la clave Ki y el algoritmo A3 para generar el valor SRES.
2. La red le envía el número aleatorio RAND al móvil.
3. El móvil con la clave Ki, el número RAND y el mismo algoritmo A3, genera el valor SRES y se lo envía a la red.
4. La red comprueba que ambos números son iguales para permitir el acceso o no.

CIFRADO DE LAS COMUNICACIONES:

Este apartado es el encargado de que cuando se produzca un uso de la red por parte del abonado, si se interceptan las comunicaciones radio, éstas no puedan ser leídas por el que las intercepta. En otras palabras, las comunicaciones se mantienen confidenciales entre móvil y BTS.

Para el cifrado de las comunicaciones de hace uso de otra clave, Kc, que genera el AuC al producirse la autenticación del móvil en la red. Como esta clave es diferente en cada acceso del móvil a la red. Al generarse en el AuC mediante el algoritmo A8, la tarjeta SIM también la genera con el mismo algoritmo, ya que dispone del número RAND y de la clave Ki como el AuC. De esta forma se evita enviar dicha clave por el enlace radio.

También hace uso de otro algoritmo, A5/$n$ con $n$ de 1 a 7, que es el utilizado para cifrar los bits transmitidos.




**33. PROCEDIMIENTO DE CIFRADO DE LAS COMUNICACIONES**

## 2.5 SISTEMA GPRS

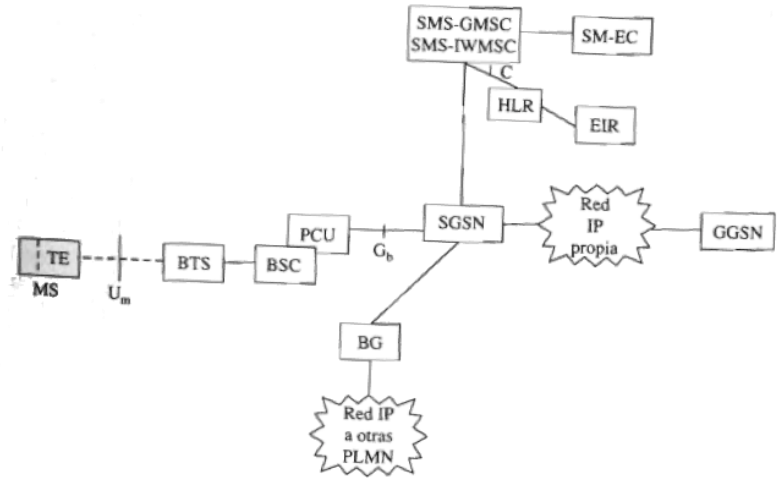
El sistema GPRS es un sistema de transmisión de datos en redes móviles. Para conseguir su objetivo utiliza cuatro mecanismos:

- Esquemas de codificación mejorados respecto a los de GSM.
- Posibilidad de utilizar diferentes *slots* temporales para una comunicación y funcionamiento de forma independiente de los enlaces ascendentes y descendentes.
- Compartir recursos radio entre varios usuarios.
- Conmutación de paquetes tanto en el enlace radio como en la red.

Gracias a estos mecanismos, GPRS es capaz de ofrecer al usuario:

- Conexión a redes de paquetes.
- Soporte de aplicaciones TCP/IP y X.25.
- Conectividad permanente.
- Eliminación de limitaciones en el servicio de mensajería.
- Diferentes parámetros de calidad de servicio.
- Facturación por volumen de datos y no por tiempo.

Para llevar a cabo todo esto, es necesario un cambio radical en el núcleo de la red, ya que ésta está preparada para la conmutación de circuitos y no para la conmutación de paquetes. Por ello se añaden equipos nuevos a la arquitectura, que son el SGSN (*Serving GPRS Support Node*) para le gestión de usuarios y encaminamiento de paquetes, el GGSN (*Gateway GPRS Support Node*) que es la pasarela entre la red móvil y el resto de redes de datos y el PCU (*Packet Control Unit*) para la gestión de paquetes por parte de las BSC.




**34. ARQUITECTURA GPRS**

En cuanto a la interfaz radio, se crean nuevas estructuras de canales físicos y canales lógicos para la transmisión de paquetes y señalización asociada a ellos. Se crea un nuevo canal físico, PDCH (*Packet Data CHannel*), donde se encapsulan los canales lógicos de datos.

Los canales lógicos comunes de GPRS son:

- PBCCH: *Packet Broadcast Control CHannel*, en el que la BTS transmite información general sobre la red y la celda.
- PCCCH*: Packet Common Control CHannel* compuesto por los siguientes canales:

- PPCH: *Packet Paging CHannel*, por donde la BTS avisa de la llegada de paquetes.
- PRACH: *Packer Random Access CHannel*, usado de forma similar al canal RACH de GSM, para peticiones de los móviles a la BTS.
- PAGCH: *Packet Access Grant CHannel*, empleado por la red para facilitar al MS los recursos radio solicitados.
- PNCH: *Packet Notification CHannel*, usado por la red en comunicaciones punto a multipunto.

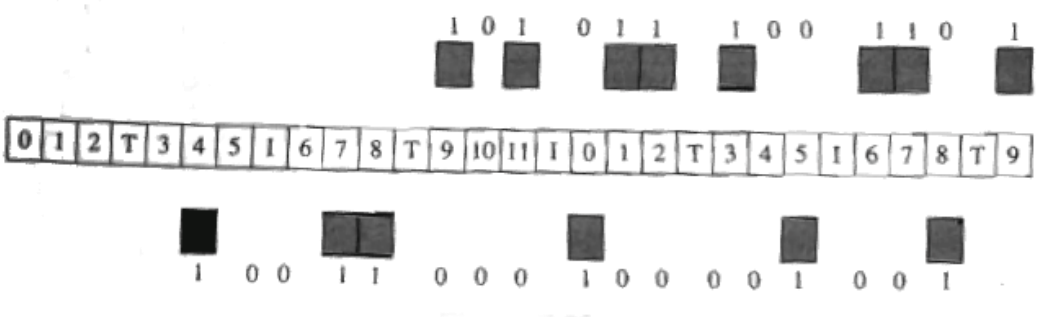
Los canales dedicados en GPRS son:

- PDTCH: *Packet Data Traffic CHannel*, canal bidireccional de tráfico de paquetes.
- Canales de control asociados:
  - PACCH: *Packet Associated Control CHannel*, canal bidireccional para señalización asociada a una transmisión de paquetes.
  - PTCCH: *Packet Time advance Control CHannel*, canal bidireccional para regular la temporización de los paquetes.

Una de las características de GPRS es que los recursos radio se comparten entre los diferentes usuarios, ya que son transmisiones discontinuas. Aparece el concepto de TBF (*Temporary Block Flow*) que es cada conexión unidireccional para la transmisión de paquetes. Un móvil puede tener un TBF asignado para el enlace ascendente y otro diferente para el descendente, permitiendo la asignación asimétrica para ambas direcciones. Cada TBF tiene un identificador temporal TFI (*Temporary Flow Identity*) usado para poder distinguir a qué conexión pertenece un paquete.

A la hora de enviar los paquetes en el enlace descendente, no hay problemas de colisión al haber un único emisor. Pero en el caso del enlace ascendente sí pueden aparecer problemas de colisiones. Para evitarlo, GPRS regula el acceso:

- Asignación fija: La PCU asigna a cada MS un mapa de bits, es decir, períodos en los que podrá transmitir y en los que no, ya que habrá otros MSs transmitiendo en el mismo TS.




**35. MAPEO DE ASIGNACION DE TS PARA GPRS**

En la figura anterior se observa el acceso al enlace ascendente en el mismo TS para dos MSs diferentes, cada uno con su mapa de bits de transmisión.

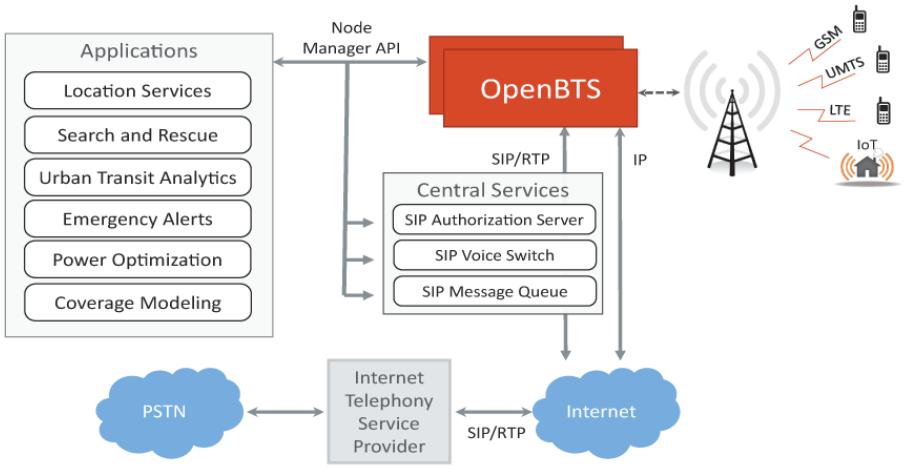
- Asignación dinámica: En este caso no existe un mapa fijo como en el caso anterior, sino que en este caso la regulación del acceso se realiza mediante el parámetro USF (*Uplink State Flag*), asignado a un MS concreto. Todos los móviles pueden leer el valor USF de los bloques radio, por lo que cuando el móvil con el USF *N* lee ese valor (*N*) puede transmitir en el bloque radio (*k*+1)-ésimo. El USF dispone de 3 bits, permitiendo compartir un TS por hasta ocho móviles.

# 3. SISTEMA PROPUESTO

**36. LOGOTIPO DE LA IMPLEMENTACIÓN COMERCIAL DE OPENBTS [13]**

En este tercer capítulo se realizará una exposición del sistema propuesto como alternativa a la actual arquitectura de red GSM. Una vez vista la arquitectura a desplegar se mostrará una descripción detallada tanto de la parte hardware como de la parte software del sistema. El capítulo finalizará con la explicación de cómo se encaminan las llamadas por la centralita software desde y hacia los móviles y el exterior de la red GSM, i.e. la Red Pública de Conmutación Telefónica o PTSN en sus siglas en inglés *Public Telephony Switching Network*.

## 3.1 ARQUITECTURA E INTERFACES DE LA RED MÓVIL




**37. ARQUITECTURA DESARROLLADA EN OPENBTS [14]**

### 3.1.1 COMPARATIVA CON LA RED ACTUAL GSM

En el diagrama 37. Arquitectura desarrollada en Open se puede observar cómo el sistema aquí desarrollado dispone de muchos menos elementos que la red actual GSM, así como un número mucho menor de diferentes tipos de interfaces ya que sólo necesita la interfaz entre el servidor donde esté alojado OpenBTS y el equipo radio (normalmente GigabitEthernet) y la conexión de éste con el exterior mediante una conexión IP. Sobre esta conexión se da servicio de Internet a los dispositivos móviles con GPRS y el servicio de voz viajará sobre una conexión RTP/SIP.

Esta simpleza hace que sea posible desplegar una red GSM en muy poco tiempo y con muy pocos recursos. Para aplicaciones concretas, esta arquitectura resulta mucho más eficiente que desplegar equipos estándares de GSM. La interfaz Um es la única que se mantiene intacta entre GSM tradicional y este sistema, ya que de esta forma este sistema se puede utilizar cualquier móvil GSM convencional, lo que ofrece una cuota de mercado muy amplia.

A continuación se mostrará, de forma resumida, una tabla con las equivalencias entre la red GSM estándar y la desplegada en el proyecto en cuestión:

| Interfaz/Equipo GSM estándar | Módulo correspondiente en OpenBTS | Comentarios |
|---|---|---|
| Um | Um | Es la misma interfaz para que sean compatibles |
| BTS | SDR/Trasceiver | |
| BSC | OpenBTS | |
| Abis | UDP | Conexión entre trasceiver y OpenBTS |
| MSC | Asterisk | PBX software que use SIP/RTP |
| VLR | SIP Authorisation Server | |
| HLR | SIP Authorisation Server | |
| AuC | SIP Authorisation Server | |
| EiR | SIP Authorisation Server | |
| SMS-GMSC | SMQueue | |
| SGSN | IPtables | |

**38. TABLA COMPARATIVA ENTRE GSM CONVENCIONAL Y OPENBTS**

Se puede observar que toda la parte de gestión de usuarios, mientras que en el estándar GSM necesita de diferentes equipos e interfaces (HLR, VLR, AuC, EiR), en OpenBTS, al ser toda la señalización dentro de la red mediante SIP, no requiere de tantos elementos diferentes ya que está todo centralizado en un único módulo.

## 3.2 DESCRIPCIÓN HARDWARE

A continuación mostraremos los recursos hardware utilizados para llevar a cabo el despliegue de la red GSM.

### 3.2.1 ESTACIÓN MÓVIL

La estación móvil o simplemente teléfono móvil, es el dispositivo del que disponen los abonados de la red. En el capítulo anterior se realizó una descripción genérica de estos dispositivos. En este caso se van a detallar los dispositivos que se han utilizado:

| | HTC Magic | Sony Xperia st21i | Samsumg SGH-L760V | Motorola C123 |
|---|---|---|---|---|
| Bandas de uso soportadas | GSM 850,900,1800, 1900<br>HSDPA 900,2100 | GSM 850,900,1800,1900<br>HSDPA 900,2100 | GSM 900,1800,1900<br>UMTS 900 | GSM 900,1800 |
| GPRS | Clase 10 (4+1/3+2 *slots*) | Clase 32 (5+3) | Clase 10 (4+1/3+2 *slots*) | - |
| Velocidad máxima GPRS | 32 - 48 kbps | 86 kbps | 32 - 48 kbps | - |
| OS | Android 1.6 | Android 4.0.4 | Propietario | Propietario |
| IMEI | 354059023962101 | 353809053856701 | 356603012547734 | 358317016983112 |

**39. TABLA DE DISPOSITOS MÓVILES UTILIZADOS EN EL PROTOTIPO**

### 3.2.2 TARJETA SIM

Las tarjetas que se han utilizado son aquellas desactivadas por diferentes compañías telefónicas y una genérica configurable, de una compañía china. No permiten la conexión a sus redes, pero como en nuestro caso sí tenemos el control sobre la red, podemos permitirles el acceso. Mediante el software OsmocomBB se ha obtenido mucha más información de cada tarjeta, mostrándose a continuación sólo un resumen con la información más relevante. Toda la información obtenida está en el Anexo 4 del presente documento.

| | Vodafone | Simyo | MicroSIM Simyo | China |
|---|---|---|---|---|
| MMC | 214 | 214 | 214 | 460 |
| MNC | 01 | 19 | 19 | 01 |
| MSIN | 45002081381 | 0180058966 | 0180026482 | 1901250000 |
| IMSI | 2140145002081381 | 214190180058966 | 214190180026482 | 460011901250000 |
| Ki | 00E7EC0A75843C5800 | 00A355B37C3E49EB97 | 9EB53C1A693D6AF9 | 00445DC8A15B9E9400 |
| MSISDN asignado en OpenBTS | 699666141 | 699666143 | 699666142 | 699666140 |

**40. TABLA TARJETAS SIM DE PRUEBA**

### 3.2.3 SERVIDOR LINUX

El servidor Linux utilizado es Ubuntu Server 12.04 32bits funcionando sobre una máquina virtual VirtualBox de 32 bits con cuatro núcleos (OpenBTS recomienda el uso de, al menos, dos núcleos), 512MB de RAM y un disco duro de 8GB. Tiene habilitadas 3 interfaces de red:

- Una con conexión directa al puerto Gigabit Ethernet del PC anfitrión, utilizada para la comunicación entre OpenBTS y el equipo SDR.
- Otra interfaz de red configurada como NAT para darle acceso a Internet al servidor y poder usar dicha conexión a Internet para ofrecer servicios de GPRS a los dispositivos móviles y como troncal para telefonía IP.
- La última interfaz de red está conectada solamente con el anfitrión para realizar labores de administración del equipo, acceso SFTP, y conexión VoIP con los *softphones* del PC anfitrión.

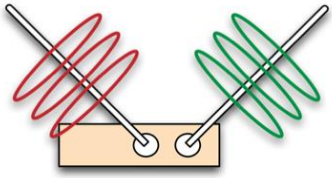
En las pruebas, dicha máquina virtual se ha ejecutado sobre un PC anfitrión con un Pentium i5 con 4Gb de RAM. Es importante que disponga de una tarjeta Gigabit Ethernet conectada de forma directa al equipo SDR. También se puede emplear un adaptador USB 3.0 – Gigabit Ethernet con buenos resultados, siempre que dicho adaptador esté conectado a un puerto USB 3.0, ya que si se conecta a un puerto USB 2.0 éste no tiene la suficiente capacidad para poder transmitir tanta información.

### 3.2.4 EQUIPO SDR

**41. EQUIPO SDR UTILIZADO PARA EL PROTOTIPO**

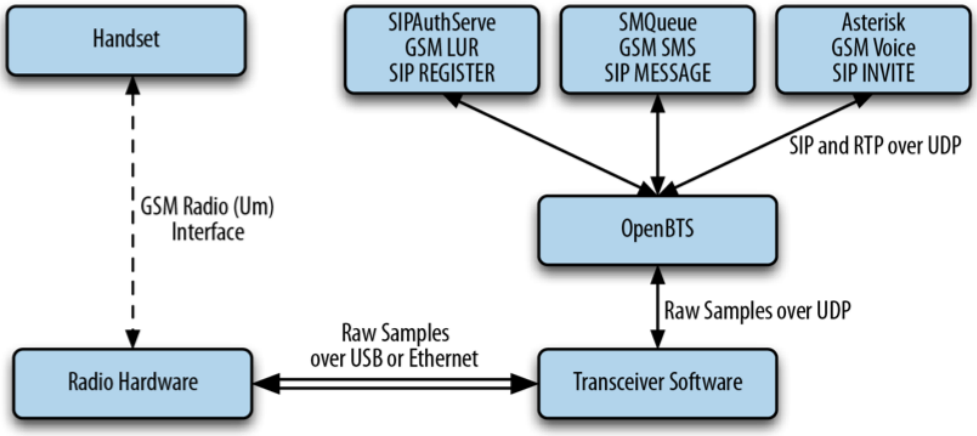
Éste es el encargado de convertir las tramas UDP, enviadas por la interfaz Gigabit Ethernet, en una emisión radioeléctrica en la parte de transmisión, así como recibir las señales de los móviles y convertir dicha señal en tramas UDP por la interfaz Gigabit Ethernet que procesará el software "*transceiver*" del servidor Linux. Concretamente se va a emplear el equipo NI USRP-2922 del fabricante National Instruments. Este equipo tiene capacidad de generar y recibir señales desde 400MHz hasta 4.4GHz y un ancho de banda de hasta 40Mhz, suficiente para trabajar con las bandas de frecuencia de GSM900 y DCS1800. Este equipo SDR se conecta directamente al PC anfitrión por una interfaz de red Gigabit Ethernet.

Para la transmisión y recepción se han empleado dos antenas dipolo diseñadas para las bandas GSM y colocadas en ángulo de 90 grados para minimizar las interferencias entre la parte transmisora y la parte receptora como se puede ver en la imagen siguiente:



**42. POSICION DE ANTENAS TX/RX PARA MINIMIZAR POSIBLES INTERFERENCIAS**

## 3.3 OPENBTS




**43. ARQUITECTURA DE OPENBTS**

Una vez descrito el hardware empleado, continuaremos con la descripción del software que se ha instalado y configurado en el servidor para poder llevar a cabo el despliegue de la red móvil.

El paquete OpenBTS consiste en diferentes programas que se ejecutan como servicios en la máquina Linux. Dichos programas son "*transceiver*", "*OpenBTS*", "*SIPAuthServe*","*NodeManager*", "*SMQueue*", "*OpenBTSCLI*" y por último, aunque no pertenece al proyecto OpenBTS, pero es necesario, "*Asterisk*".

A continuación se hará una breve descripción de cada uno de ellos.

### 3.3.1 TRANSCEIVER

Este software es el encargado de las capas uno a tres en la pila de protocolos. Se comunica directamente con OpenBTS y el equipo radio SDR mediante UDP y la interfaz GigabitEthernet.

Tiene las siguientes capacidades en su capa física:

- Radiomódem: OpenBTS y en concreto este módulo "transceiver" puede trabajar en las 4 bandas principales de GSM:
    - GSM850 y PCS1900. Utilizadas en la región 2 definida por la ITU.
    - PGSM900, EGSM900 y DCS1800. Utilizada en la mayor parte del mundo.
  - Soporta la modulación GMSK con una velocidad de símbolo de 270.833 KHz y un espaciado entre canales de 200KHz.

- Multiplexado y temporización de las señales: Como se ha visto en el capítulo dos, cada portadora dispone de hasta ocho *slots* temporales. El software se encarga de la generación de estos *slots* temporales.
- Codificación del canal: Este software también es el encargado de la corrección de errores en las tramas recibidas. Como regla general, cada canal utiliza un código de paridad de bloque, a una razón de ½, un código convolucional de cuarto orden y un entrelazado de 4 ráfagas u 8.

#### CAPA DE ENLACE

En este caso el software "*transceiver*" es el encargado de procesar también la capa dos de la pila de protocolos, que es una forma simplificada de HDLC, LAPDm.

#### CAPA DE RED

Este software participa en la capa de red, dentro de una subcapa llamada Recurso Radio, RR. Encargada de la asignación y liberación de los canales lógicos en el enlace radio.

Las combinaciones de canales lógicos soportados por el software son:

- Combinación I: TCH/F+FACCH/F+SACCH. Tráfico a máxima velocidad, pudiendo ser usada en todos los canales excepto en C0T0.
- Combinación V: FCCH+SCH+BCCD+CCCH+4 SDCCH+4 SACCH. Combinación de canales lógicos utilizados en el primer canal físico C0T0.
- Combinación VII: 8 SDCCH+8 SACCH. Utilizada en entornos donde la carga de transacciones SMS y registros es alta. Sobre todos los canales físicos excepto el C0T0.

Una de las limitaciones del sistema es que no soporta canales a media velocidad definidos en el estándar GSM.

La configuración elegida en nuestro caso es la siguiente:

- Para el canal C0T0, la combinación V.
- Para cinco *slots* temporales, la combinación I.
- Los dos *slots* temporales que quedan se reservan para GPRS.

El software termina comunicando esta subcapa con el software OpenBTS.

### 3.3.2 OPENBTS

El software OpenBTS es el encargado de realizar la traducción GSM-SIP/RTP/SQL. Se encarga del procesado de dos de las tres subcapas de la capa de red de la pila de protocolos de GSM. Dichas subcapas son:

#### GESTIÓN DE LA MOVILIDAD, MM EN SUS SIGLAS EN INGLÉS *MOBILITY MANAGEMENT*.

Encargada de autenticar a los usuarios y realizar el seguimiento de sus movimientos entre las diferentes celdas. Traduce las transacciones de movilidad en sus correspondientes transacciones SIP comunicándose con el registro de la centralita Asterisk.

#### CONTROL DE LAS LLAMADAS, CC EN SUS SIGLAS EN INGLÉS *CALL CONTROL*.

Esta subcapa se encarga de conectar las llamadas telefónicas con transacciones SIP para la centralita local Asterisk.

### 3.3.3 SIPAUTHSERVE

Uno de los conceptos clave para comprender la traducción entre GSM-SIP es que cada teléfono móvil conectado aparece en la red VoIP como un terminal SIP con el nombre de usuario

“IMSIXXXXXXXXXXXXXXX”, donde las “X” son el IMSI de la tarjeta SIM conectada al móvil. Otro parámetro como terminal SIP es la dirección IP, que será la dirección del OpenBTS al que se encuentre conectado el móvil, ya que puede haber varios OpenBTS para la misma red VoIP funcionando como Multi-BTS. OpenBTS de esta forma es totalmente transparente en la red VoIP.

El software SIPAuthServe se refiere al registro de subscriptores, es decir, cumple la función del HLR, VLR, AuC y EiR en una red GSM convencional. Es el encargado de acceder a una base de datos de SQLite3, la misma base de datos a la que accederá Asterisk para gestionar los usuarios y llamadas.

Para poder dar de alta un nuevo usuario en la red es necesario conocer, como mínimo, el IMSI de la tarjeta SIM que va a emplear. El procedimiento para obtener el IMSI se explica en el Anexo 4 del presente documento.

Con dicho IMSI podremos crear una nueva entrada en la base de datos de subscriptores y que dicho equipo pueda tener acceso a la red.

Cabe la posibilidad de no necesitar el IMSI para dar de alta a los abonados, pero para ello se debe dejar abierto el acceso a la red a todos los equipos que lo soliciten, con el consiguiente riesgo para la seguridad.

### 3.3.4 NODEMANAGER

NodeManager es una API para permitir a aplicaciones de terceros gestionar diferentes bases de datos y configuraciones del paquete OpenBTS: OpenBTS, SIPAuthServe y SMQueue. Para ello utiliza una interfaz JSON.

Un ejemplo de uso es para dar de alta un nuevo usuario en la red GSM. Una vez conocido el IMSI añadiremos el usuario al registro de subscriptores por medio de la sentencia:

```
$./nmcli.py sipauthserve subscribers create “SonyXperia” IMSI214190180058966
699666143
```

En la línea anterior se le ha indicado crear una nueva entrada en la tabla de subscriptores de la base de datos de SIPAuthServe con el nombre “SonyXperia”, el usuario IMSI214190180058966 y el MSISDN 699666143.

RECORDATORIO: El usuario será siempre “IMSIXXXXXXXXXXXXXXX”, donde las “X” son el IMSI de la tarjeta SIM conectada al móvil.

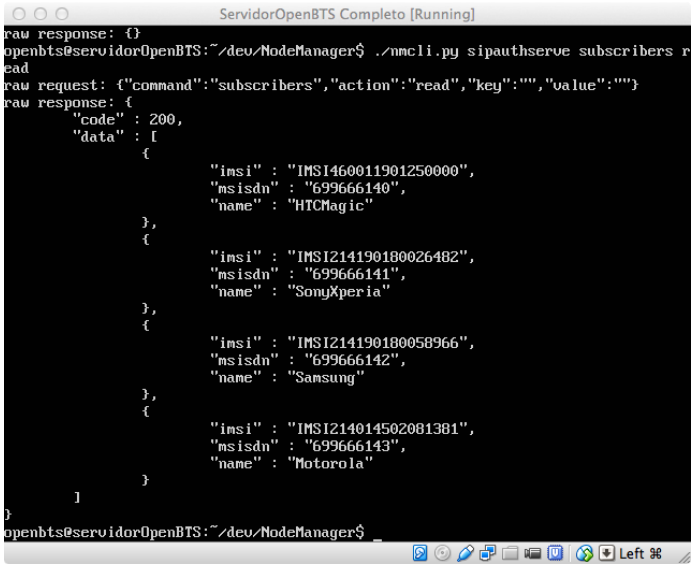
Para eliminar un usuario de la base de datos utilizamos el mismo script de NodeManager. Por ejemplo, para eliminar el usuario anterior:

```
$./nmcli.py sipauthserve subscribers remove “imsi” IMSI214190180058966
```

Si queremos mostrar la lista con todos los subscriptores que hay dados de alta en el sistema ejecutamos:

```
$./nmcli.py sipauthserve subscribers read
```

Y obtenemos como respuesta:




**44. EJEMPLO DE ABONADOS EN LA BASE DE DATOS**

### 3.3.5 SMQUEUE

El sistema GSM permite, además de la transmisión de voz, el envío y recepción de mensajes de texto cortos o SMS. Este envío y recepción de mensajes está basado en la filosofía de almacenamiento y reenvío. OpenBTS implementa esta funcionalidad mediante este software, SMQueue, que no es más que una cola a la que le llegan los mensajes y va intentando enviarlos, hasta que llegan a su destino o hasta que se descartan porque el destino es inalcanzable. Su funcionamiento es similar al de un servidor de correo electrónico.

Puede utilizar dos tipos de direcciones, ISDM/E.164 numéricas y nombres de usuario SIP. Toda aquella dirección no numérica trata de resolverla como nombre de usuario SIP.

Dispone de diferentes aplicaciones de mensajes, en las cuales un mensaje enviado hace las veces de argumento para una función, permitiendo la creación de aplicaciones interactivas vía SMS. Las dos aplicaciones más interesantes que trae SMQueue por defecto son:

- Info (411): Un mensaje de texto enviado al número 411 devuelve al emisor el mismo texto, junto con información acerca del estado de SMQueue. Uno de los datos importantes recibidos es el IMSI del emisor.
- *Autoprovisioning* o registro (101): Esta aplicación permite a un usuario dar de alta su terminal en la base de datos de abonados. El emisor envía el número de teléfono deseado y, si está libre y tiene un mínimo de cifras, la aplicación creará el registro en la base de datos de subscriptores de forma automática. NOTA: Para que esta aplicación sea útil, OpenBTS deberá estar configurado para permitir que todos los móviles se puedan registrar.

### 3.3.6 OPENBTSCLI

Este es el último software dentro del paquete OpenBTS. Es un software para gestionar todas las configuraciones de la BTS así como para poder monitorizar el estado de la misma. Al instalar OpenBTS, este gestor se instala en la carpeta principal de OpenBTS y también una copia en la carpeta personal del usuario “openbts”. La forma más sencilla de acceder a él es ejecutándola desde la carpeta personal:

```
openbts@openbts$ sudo ./CLI
```

Al ejecutarlo obtendremos un terminal de la forma:

```
OpenBTS>
```

Con él podremos configurar todos los parámetros de nuestra estación base, así como enviar SMS, ver los canales activos, la carga de uso de la BTS, modificar parámetro de la interfaz radio (potencia de emisión, sensibilidad del receptor…), etcétera. También podremos monitorizar las llamadas en curso y colgarlas en caso de que sea necesario.

Para ver la configuración de un parámetro cualquiera pondremos:

```
OpenBTS> config GSM.Radio.C0
```

Con esto podremos ver en que ARFCN está emitiendo nuestra estación base. Si después del comando escribimos algo, entonces lo que hacemos el modificar el valor que tenía al nuevo valor. Por ejemplo para asignar nuestro ARFCN=1 pondríamos:

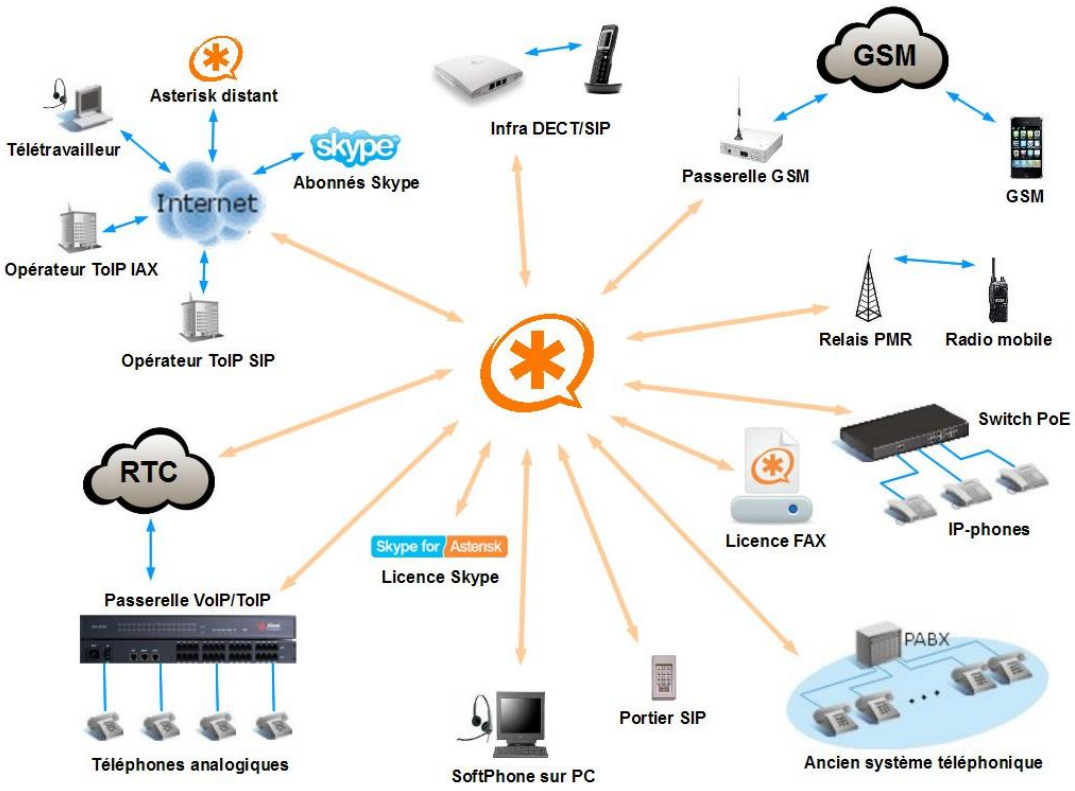
```
OpenBTS> config GSM.Radio.C0 1
```

Y para volver a la configuración por defecto, usamos la palabra "*unconfig*" seguida de la configuración que queremos que vuelva a ser la original. Por ejemplo, para volver al ARFCN por defecto, sería:

```
OpenBTS> unconfig GSM.Radio.C0
```

Para ver todos los comandos disponibles, escribimos "*help*" en la línea y nos mostrará el listado completo. Una explicación detallada de cada uno la podemos ver en el apéndice C del manual de usuario de OpenBTS V4.0 junto a todos los posibles parámetros de configuración y su explicación, en el apéndice B del mismo documento.

## 3.4 ASTERISK




**45. ASTERISK Y SU NUBE DE POSIBILIDADES DE INTERCONEXIÓN**

### 3.4.1 INTRODUCCIÓN

Asterisk es una centralita telefónica virtual. En nuestro caso hace el papel de MSC, ya que es la encargada de encaminar las llamadas entre los diferentes usuarios mediante voz sobre IP. Los usuarios se conectan a ella mediante el protocolo SIP o IAX. En el caso de OpenBTS, cada usuario es un usuario SIP.

Está diseñada de forma completamente modular, de manera que sólo instalas los módulos que necesites para tu aplicación. OpenBTS trae por defecto una versión de Asterisk junto con un paquete de configuración automático, haciendo mucho más sencilla su configuración. Puesto que el registro de usuarios está en una base de datos externa a Asterisk, en principio necesitaría de módulos adicionales para poder acceder a dicha base de datos. Sin embargo, con esta solución en un único paquete, la configuración es automática.

### 3.4.2 GESTIÓN DE USUARIOS

La gestión de usuarios se realiza en el archivo /etc/asterisk/sip.conf. Este archivo permite definir los usuarios que pueden acceder a la centralita. Para el caso en cuestión, OpenBTS incluye un paquete de configuración en su instalación, de forma que una vez instalado, Asterisk queda configurado para la realización y envío de llamadas. La instalación modifica los archivos principales, sip.conf y extensions.conf.

Dentro del archivo principal sip.conf encontramos la siguiente configuración relevante:

```
[CodecBTS](!)
        disallow=all      ; need to disallow=all before we can use allow
        allow=gsm                 ; GSM
        allow=ulaw                ; ISDN US
        allow=alaw                ; ISDN EU
```

```
[optionsBTS](!)
        type=peer
        context=from-openBTS
        dtmfmode=rfc2833
        canreinvite=no
        qualify=no                ; openbts do not support OPTION
        insecure=port,invite
```

Estas dos configuraciones nos indican los códecs que va a utilizar OpenBTS y el tipo de usuario que es un teléfono móvil. Después, en el archivo /etc/asterisk/sip-custom-context.conf se definen los diferentes usuarios SIP. Uno de ellos es el necesario para reconocer a OpenBTS:

```
[00101100010](optionsBTS,CodecBTS)        ;default account for when openBTS
and MSC is on the same server
        host=localhost
        port=5062
```

En el caso de disponer de un servicio troncal de llamadas VoIP, como es nuestro caso, agregaremos la troncal en este archivo:

```
[netelip]
type=friend
username=<Ususario_troncal>
context=default
host=<servidor_troncal>
canreinvite=no
secret=<contraseña_de_la_troncal>
nat=force_rport,comedia
fromdomain=<dominio_troncal>
disallow=all
allow=alaw
insecure=very
fromuser=<Ususario_troncal>
```

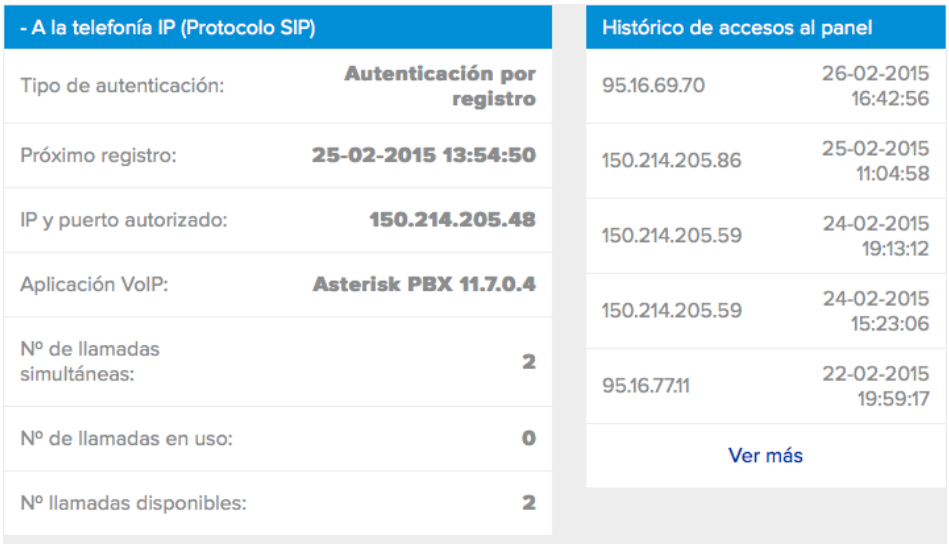
En nuestro caso el proveedor de servicios VoIP es *Netelip* y, para poder conectarnos a él, deberemos añadirlo como un usuario SIP más.

**46. SERVICIO TRONCAL SIP CONRATADO**

También deberemos indicar a Asterisk que se registre en el servidor SIP de nuestra troncal. Para ello, en el archivo /etc/asterisk/sip-custom-register.conf indicaremos que se registre:

```
register => INSERT_YOUR_ACCOUNT:INSERT_YOUR_PASSWORD@sip.netelip.com
```

Una vez tenemos configurados los usuarios SIP, podemos ver si ha conectado de forma correcta a nuestro proveedor de servicios. En nuestro caso, dicho proveedor dispone de un panel web donde gestionar todos los servicios ofrecidos. Uno de ellos es un registro de conexiones:




**47. DETALLES DEL LOG DE CONEXION AL SERVCIO TRONCAL**

En él que se puede comprobar, al ver el panel de históricos, que se ha realizado una conexión desde nuestro servidor Asterisk.

### 3.4.3 PLAN DE LLAMADAS

Una vez configurados los usuarios SIP, hay que configurar el plan de marcación. El plan de llamadas está organizado en lo que se llaman contextos. Cada usuario dispone de un contexto, y es dicho contexto el que determina qué hacer cuando el usuario realiza una llamada.

Un ejemplo de contexto sencillo, es el siguiente, en el que el usuario al que está asociado puede realizar llamadas:

```
[mi-contexto]
exten => 1004,1,Dial(SIP/1004,60) ;Para llamar al 1004
exten => 1004,n,Hangup()          ;Un vez finalizada la llamada cuelga
```

Los contextos se ejecutan de forma secuencial, de forma que cuando un usuario tenga asignado el contexto “mi-contexto” sólo podrá llamar al 1004. Cuando éste usuario llame al 1004, primero se realizará la llamada como tal (primera línea, Dial(SIP/1004,60)). Una vez ha terminado la llamada o han pasado 60 segundos sin contestación, se ejecuta la siguiente línea, que consiste en finalizar la llamada.

Los contextos se definen entre corchetes, y después se indican las acciones a realizar con el siguiente formato:

```
exten => <extensión_marcada_por_usuario>,<prioridad>,<Aplicación a ejecutar>
```

La extensión marcada por el usuario puede ser la extensión directamente, como en el caso anterior, o una expresión regular, ya que si tenemos decenas de extensiones, escribir lo mismo para todas ellas no es productivo y es difícil de mantener el plan de marcación. Para usar una expresión regular se empieza por el carácter '_' seguido de la expresión. Por ejemplo, en el contexto anterior, si queremos que el usuario pueda llamar a todas las extensiones que comienzan por 1 y tienen 4 cifras se pondría de la siguiente forma:

```
[mi-contexto]
exten => _1XXX,1,Dial(SIP/${EXTEN},60)
same  =>       n,Hangup()
```

Se puede ver cómo la extensión en este caso indica que es un patrón, de cuatro cifras, siendo la primera un 1 y las tres restantes un número entre 0 y 9. Otra diferencia es el uso de la variable ${EXTEN} que almacena la extensión marcada por el usuario. De esta forma le indicamos a la aplicación *Dial* que llame al usuario SIP indicado por la extensión que ha marcado.

Para no tener que poner la extensión en cada línea, se puede utilizar la palabra "*same*", que indica que, para esa misma extensión, cuando termine de ejecutar la línea pase a la siguiente.

Volviendo a nuestro sistema, OpenBTS configura de forma automática el plan de llamadas. Es decir, una vez instalado todo el sistema y dados de alta los diferentes móviles mediante la aplicación de NodeManager, éstos podrán realizar llamadas entre ellos sin problemas. Si queremos que puedan realizar llamadas al exterior haciendo uso del proveedor configurado, deberemos añadirlo al archivo /etc/asterisk/extensions.conf la línea siguiente:

```
[globals](+)
GW1=netelip      ;Primary sip account used for handeling calls to the PSTN,
change the name to match sip.conf
```

En nuestro caso la troncal es "netelip". Asterisk, cuando un móvil realiza una llamada a un móvil dentro de la red creada, primero realiza una búsqueda del número marcado dentro de la red. Si está en ella, llama a dicho terminal y, si el número es desconocido, lo encamina al contexto de llamadas externas.

Una vez configurados los usuarios y el plan de llamadas, para que los cambios realizados surtan efecto hay dos opciones, reiniciar el servicio Asterisk, o acceder a su terminal y recargar ambos archivos.

Para acceder a su consola de configuración escribimos:

```
sudo asterisk –r
```

Dentro del intérprete de comandos, los dos comandos para recargar los usuarios y plan de marcación son:

`sip reload`: recarga el archivo sip.conf

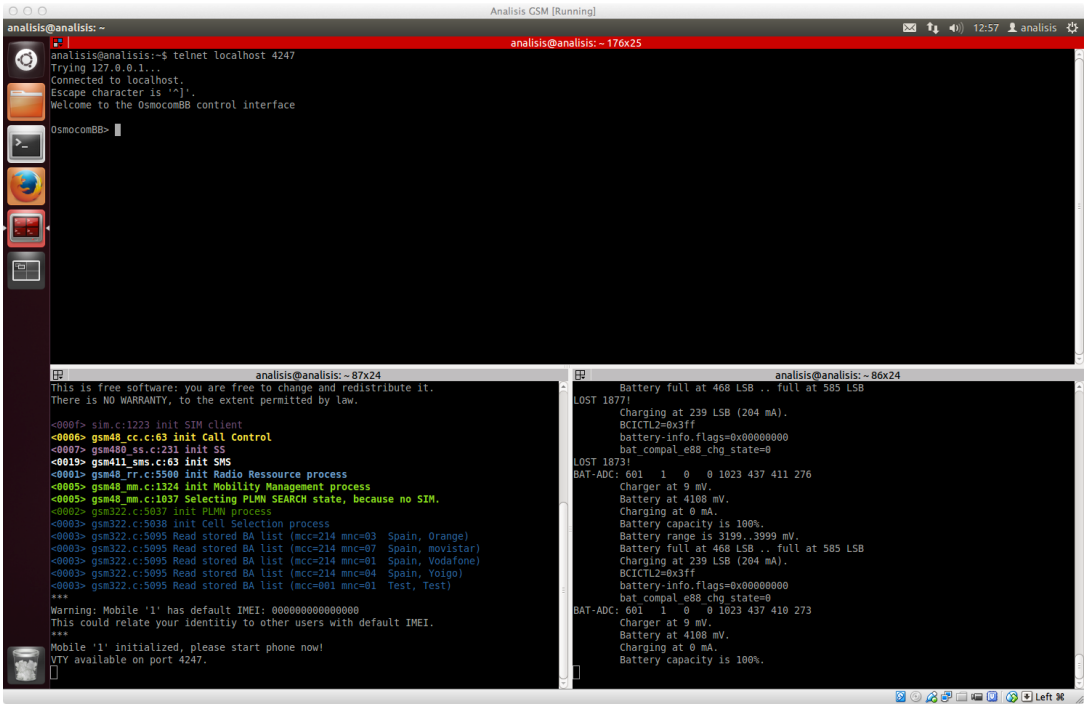
`dialplan reload`: para recargar el plan de marcado, cuando hacemos modificaciones en el archivo extensions.conf

Una vez recargados los usuarios y el plan de llamadas en Asterisk junto con OpenBTS, dispondremos de la estación base configurada para poder realizar llamadas entre los usuarios de la red y que éstos puedan realizar llamadas al exterior. No se contempla la posibilidad de que desde el exterior llamen a los teléfonos de nuestra red, ya que para ello se debería pedir licencia a la comisión nacional del mercado de las telecomunicaciones para que nos asigne un conjunto de números de teléfono.

## 3.5 SISTEMA OSMOCOMBB

Este software nos permite disponer de un teléfono móvil en el que la capa física está implementada en el firmware modificado de un teléfono móvil y el resto de capas de la pila GSM están implementadas por software. Al final del presente documento, hay un anexo dedicado a la instalación de este sistema en un PC Linux. Aquí explicaremos su uso una vez instalado para poder conectarnos a la red GSM creada por nosotros o cualquier otra red GSM. La instalación se explica en el Anexo 3 del presente documento.

Tras la puesta en marcha del sistema completo, obtenemos un terminal de la forma:




**48. TERMINALES LIUNX PARA EL CONTROL DEL SISTEMA OSMOCOMBB**

Donde los dos terminales de la parte inferior sólo muestran los mensajes de diagnóstico del firmware y la aplicación "*mobile*". El terminal superior es en el que podremos comenzar a operar. El modo de funcionamiento es similar al terminal de configuración de dispositivos Cisco. Para ver los comandos disponibles escribimos "?" (sin comillas) obteniendo en el primer nivel los siguientes comandos posibles:

```
OsmocomBB>
show       Show running system information
list       Print command list
exit       Exit current mode and down to previous mode
help       Description of the interactive help system
enable     Turn on privileged mode command
terminal   Set terminal line parameters
who        Display who is on vty
monitor    Monitor...
no         Negate a command or set its defaults
OsmocomBB>
```

Para poder empezar a trabajar habilitamos el modo privilegiado escribiendo:

```
OsmocomBB> enable
OsmocomBB#
```

Vemos que el terminal ha cambiado para indicar que estamos en el modo privilegiado. En este modo vemos ahora los posibles comandos:

```
OsmocomBB#
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
disable    Turn off privileged mode command
configure  Configuration from vty interface
copy       Copy configuration
terminal   Set terminal line parameters
who        Display who is on vty
monitor    Monitor...
no         Negate a command or set its defaults
off        Turn mobiles off (shutdown) and exit
sim        SIM actions
network    Network ...
call       Make a call
sms        Send an SMS
service    Send a Supplementary Service request
test       Manually trigger cell re-selection
delete     Delete
OsmocomBB#
```

Este modo privilegiado ya vemos que es mucho más interesante, ya que podemos realizar llamadas y enviar SMS. En caso de escribir un comando y que esté incompleto el sistema nos lo indicará. Para obtener ayuda del mismo, escribimos el comando seguido de la interrogación:

```
OsmocomBB# configure
% Command incomplete.
OsmocomBB# configure ?
terminal  Configuration terminal
OsmocomBB# configure terminal
OsmocomBB(config)#
```

Ahora estaríamos en condiciones de poder configurar nuestro terminal.

```
OsmocomBB(config)#
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.
hostname      Set system's network name
no            Negate a command or set its defaults
password      Assign the terminal connection password
enable        Modify enable password parameters
banner        Set banner string
service       Set up miscellaneous service
line          Configure a terminal line
gps           GPS receiver
hide-default  Hide most default values in config to make it more compact
ms            Select a mobile station to configure
OsmocomBB(config)#
```

Para configurar nuestro móvil vamos al menú que nos da acceso a la configuración del mismo:

```
OsmocomBB(config)# ms 1
OsmocomBB(ms)#
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.
layer2-socket       Define socket path to connect between layer 2 and layer 1
sap-socket                Define socket path to connect to SIM reader
sim                       Set SIM card to attach when powering on
network-selection-mode    Set network selection mode
imei                      Set IMEI (enter without control digit)
imei-fixed                Use fixed IMEI on every power on
imei-random               Use random IMEI on every power on
no                        Negate a command or set its defaults
emergency-imsi            Use special IMSI for emergency calls
sms-service-center        Use Service center address for outgoing SMS
call-waiting              Allow waiting calls
auto-answer               Enable auto-answering calls
force-rekey               Enable key renew forcing after every event
clip                      Force caller ID presentation
clir                      Force caller ID restriction
tx-power                  Set the way to choose transmit power
simulated-delay           Simulate a lower or higher distance from the BTS
stick                     Stick to the given cell
location-updating         Allow location updating
codec                     Enable codec
abbrev                    Store given abbreviation number
test-sim                  Configure test SIM emulation
neighbour-measurement     Allow neighbour cell measurement in idle mode
support                   Define supported features
shutdown                  Shut down and deactivate MS
OsmocomBB(ms)#
```

Como se puede comprobar, disponemos de muchas más opciones que si utilizamos un teléfono móvil convencional. Un aspecto interesante es poder utilizar una tarjeta SIM virtual, de modo que es completamente programable. Dentro del menú del teléfono móvil, nos vamos a la configuración test-sim:

```
OsmocomBB(ms)# test-sim
OsmocomBB(test-sim)#
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.
imsi            Set IMSI on test card
ki              Set Key (Kc) on test card
barred-access   Allow access to barred cells
no              Negate a command or set its defaults
rplmn           Set Registered PLMN
hplmn-search    Set Home PLMN search mode
OsmocomBB(test-sim)#
```

Si conocemos el IMSI y la Ki de una tarjeta SIM podremos hacer un clon de la misma y conectarnos a la red GSM haciéndonos pasar por dicha SIM.

Una vez visto de forma breve las posibilidades del software, pasaremos a realizar una llamada con él. Volvemos al modo privilegiado:

```
OsmocomBB# call
% Command incomplete.
OsmocomBB# call 1
NUMBER     Phone number to call (Use digits '0123456789*#abc', and '+' to dial
international)
emergency  Make an emergency call
answer     Answer an incomming call
hangup     Hangup a call
hold       Hold current active call
retrieve   Retrieve call on hold
dtmf       One or more DTMF digits to transmit
OsmocomBB# call 1 699666140
```

Al realizar la llamada, en el terminal de diagnóstico de "*mobile*" obtenemos:

```
<0009> mnccms.c:570 Make call to 699666140
<0009> mnccms.c:150  support TCH/H also
<0009> mnccms.c:174  support full rate v2
<0009> mnccms.c:178  support full rate v1
<0009> mnccms.c:187  support half rate v1
```

Para el envío de SMS se procede de forma similar a las llamadas:

```
OsmocomBB# sms 1 699666140  "Hola desde OsmocomBB"
```

# 4. RESULTADOS OBTENIDOS

En este cuarto capítulo describiremos los resultados obtenidos tras configurar todo el sistema. Comenzaremos con un breve análisis de la banda GSM en la zona en la que se han realizado las pruebas. Una vez visto los canales que hay libres, aquellos en los que si emitimos algo, con muy baja potencia y durante muy poco tiempo, no crearemos problemas a los operadores móviles que disponen de licencia, pasaremos a estudiar la parte radio del sistema, describiendo el equipo de medida utilizado y ver los resultados obtenidos con el equipo de medida, dentro de las posibilidades del equipo de medida. Una vez comprobada que la emisión por parte de OpenBTS se acerca a la teoría, procederemos a mostrar el intercambio de mensajes entre estación base y equipo móvil en diferentes escenarios: acceso a la red, realización de llamadas, envío y recepción de SMS, para ello se hará uso de un mecanismo de captura de paquetes por parte de OpenBTS para la parte de la red y por parte de OsmocomBB para la parte del móvil.

## 4.1 ANÁLISIS DE LOS CANALES EN USO EN LA ZONA DE TEST

Antes de comenzar a poner en marcha la estación base, se ha realizado un análisis de las bandas que están en uso en la zona. Para ello comenzaremos visitando la página web del gobierno, en la que se pueden ver las ubicaciones de las antenas móviles cerca de la zona de interés:

https://geoportal.minetur.gob.es/VCTEL/vcne.do

**49. PAGINA WEB DEL MINISTERIO CON INFORMACIÓN DE LAS ANTENAS DE TELEFONÍA MÓVIL INSTALADAS CERCA DE LA ETSIIT**

Se puede ver en la captura que cerca del edificio del CITIC hay 4 estaciones base. Al obtener el detalle de cada torre, obtenemos la siguiente información:

Niveles de Exposición

GOBIERNO DE ESPAÑA · MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO · SECRETARÍA DE ESTADO DE TELECOMUNICACIONES Y PARA LA SOCIEDAD DE LA INFORMACIÓN · Infoantenas

ESTACIONES DE TELEFONÍA MÓVIL

LOCALIZACIÓN

| Código | Dirección |
|---|---|
| VODAFONE ESPAÑA, S.A. - 001638 | AV ANDALUCIA, 103. GRANADA, GRANADA |

CARACTERISTICAS TÉCNICAS

| Operador | Referencia | Banda Asignada (MHz) |
|---|---|---|
| VODAFONE ESPAÑA, S.A. | GRGR-0900051 | 1905.00 - 1910.00; 2140.00 - 2155.00 |
| VODAFONE ESPAÑA, S.A. | GRGR-0900052 | 948.90 - 959.90 |
| VODAFONE ESPAÑA, S.A. | GRGR-0900053 | 1825.10 - 1845.10 |

NIVELES MEDIDOS EN EL ENTORNO

Los niveles medidos cumplen la normativa legal vigente, al encontrarse muy por debajo de los niveles de referencia establecidos.

El nivel de referencia más restrictivo para los servicios de radiocomunicación es de 200 μW/cm². El nivel de referencia para los distintos servicios de telefonía móvil es siempre superior al valor más restrictivo (200 μW/cm²) anteriormente indicado. Por ejemplo, para el servicio de telefonía móvil en la frecuencia de 2000 MHz, el nivel de referencia es 1000 μW/cm².

| Distancia (m) | (*) Acimut (°) | Valor Medido (μW/cm²) |
|---|---|---|
| 124.0 | 207.0 | 0.03066 |
| 74.0 | 145.0 | 0.06899 |
| 130.0 | 192.0 | 0.25475 |

(*) Acimut es el ángulo que tiene una determinada dirección. Para calcularlo se toma como referencia el norte geográfico y a partir de ahí se gira en el sentido de las agujas del reloj.

Gobierno de España. Ministerio de Industria, Energía y Turismo. Pº de la Castellana 160, C.P. 28046 Madrid.
Teléfono: 91 349 46 40 | 902 446 006

**50. DETALLE DE LAS ANTENAS CERCANAS A LA ETSIIT**

Tomaremos como base las medidas de potencia ofrecidas por la web del Ministerio, estas medidas han sido tomadas a una distancia fija del emplazamiento de las antenas. Para nuestro proyecto, visualizaremos el espectro en ambas bandas, pero en nuestro laboratorio, localizado en el CITIC, que es el Centro de Investigación de Tecnologías de la Información y Comunicaciones dependiente de la Universidad de Granada en el que se ha montado el prototipo de BTS.

### 4.1.1 BANDA GSM900

A continuación se muestra una tabla con aquellas estaciones que transmiten en la banda GSM900 que están cerca del CITIC. Los valores de potencia son los oficiales según la web del Ministerio, medidos en un entorno de la estación base:

| Operador | Referencia estación | Banda asignada(MHz) | Valor de potencia μW/cm² |
|---|---|---|---|
| Vodafone España S.A | GRGR-0900052 | 948.90-959.90 | 0.06899 |
| Vodafone España S.A | GRGR-1300110 | 948.90-959.90 | 0.14921 |
| Vodafone España S.A | GRGR-1200196 | 948.90-959.90 | 0.52736 |
| Vodafone España S.A | GRGR-1200197 | 948.90-959.90 | 0.52736 |
| ORANGE ESPAGNE, SAU | GRGR-0700033 | 925.10 - 935.10 | 0.35080 |
| ORANGE ESPAGNE, SAU | GRGR-1200336 | 925.10 - 935.10 | 0.35080 |
| TELEFÓNICA MOVILES ESPAÑA SAU | GRGR-0430846 | 935.10 - 948.90 | 0,41447 |

**51. OPERADORES Y BANDA ASIGNADA EN GSM900**

Tenemos la banda GSM completa por los 3 operadores. La diferencia está en el número de estaciones que tiene cada operador cerca de la ETSIIT, mientras Vodafone España S.A tiene 4 estaciones, los otros dos operadores disponen de dos y una, aparte la distancia a las estaciones móviles de éstos últimos son mucho mayores que para el caso de Vodafone. Se encuentran por lo tanto más canales libres en la parte baja de la banda, ya que está ocupada por los operadores con las estaciones más alejadas.

Tras comprobar los canales ocupados con un analizador de espectros, observamos que, como se esperaba, la zona más baja de la banda está libre, por lo tanto utilizaremos un canal, o ARFCN lo

más bajo posible, concretamente el canal 2 con una frecuencia de portadora de 935.4MHz. Aunque en la tabla anterior se muestra que ese canal está siendo utilizado por Telefónica, y parece que emite con mayor potencia, al estar la estación base más alejada que el resto, ese canal aparece como vacío cuando se toman medida con el analizador de espectros.

La configuración de la banda y canal en OpenBTS se realiza haciendo uso del cliente, y una vez dentro, con los siguientes comandos:

```
OpenBTS> config GSM.Radio.C0 2      #Indicamos usar el canal ARFCN 2, 935.4Mhz
OpenBTS> config GSM.Radio.Band 900  #Indicamos que la banda de emisión es la
de 900MHz
```

### 4.1.2 BANDA DCS1800

Para esta banda se va a realizar el mismo estudio que para el caso de GSM900, para ver las zona más libres según la información oficial del ministerio, y según las medidas tomadas en local con el analizador de espectros.

Potencia emitida según la web del Ministerio:

| Operador | Referencia estación | Banda asignada(MHz) | Valor de potencia $\mu W/cm^2$ |
|---|---|---|---|
| ORANGE ESPAGNE, SAU | GRGR-0430585 | 1859.90 - 1879.90 | 0.35080 |
| VODAFONE ESPAÑA, S.A. | GRGR-1400201 | 1825.10 - 1845.10 | 0.83103 |
| TELEFONICA MOVILES ESPAÑA SAU | GRGR-0800359 | 1805.10 - 1825.10 | 1.73840 |
| XFERA MOVILES SA | GRGR-1200127 | 1845.10 - 1859.90 | 0.63728 |

De nuevo, como en el caso de la banda GSM900, aunque la banda que ocupa Telefónica Móviles es la que emite con mayor potencia, dicha potencia está tomada a una distancia fija de la estación base. En nuestro laboratorio, aparece como libre esa banda, ya que es la que está a mayor distancia. Por lo tanto decidimos utilizar el segundo canal en la banda DCS1800:

```
OpenBTS> config GSM.Radio.C0 512        #Indicamos usar el canal ARFCN 512,
1805.2Mhz
OpenBTS> config GSM.Radio.Band 1800  #Indicamos que la banda de emisión es la
de 1800MHz
```

## 4.2 EQUIPO UTILIZADO PARA OBTENER LAS DIFERENTES MEDIDAS

Se han utilizado diferentes equipos para comprobar el funcionamiento de la red GSM. Para la parte de la interfaz radio se ha empleado un analizador vectorial y para la parte del diálogo entre estación base y móvil, se analizarán las trazas GSMTAP generadas por OpenBTS para la parte de estación base y por OsmocomBB para la parte de teléfono móvil.

### 4.2.1 ANALIZADOR VECTORIAL

El analizador vectorial utilizado es el modelo EXA del fabricante Agilent, en concreto el modelo N9010A. Dispone de un ancho de banda de 3.6GHz, suficiente para cubrir las 4 bandas más comunes del estándar GSM. Dispone de diferentes programas específicos para demodulación digital, capaces de trabajar con GSM y suficiente para nuestros propósitos.

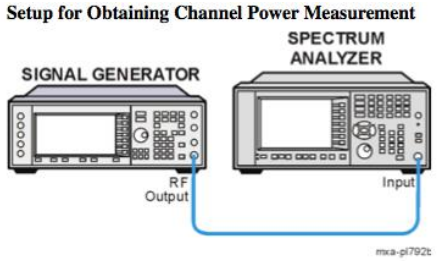
El sistema se ha comprobado tanto para la banda de 900MHz como para la de 1800MHz. De esta forma podremos ver si el equipo SDR se comporta de igual forma para una banda de menor frecuencia que para una de mayor y ver la calidad del enlace descendente para ambas bandas.

Para el caso del enlace ascendente, se han tomado medias de los slot temporales cuando hay un móvil cursando una llamada, cuando hay dos, tres, cuatro y hasta cinco llamadas cursándose a la vez, para ver los slot temporales que ocupa cada llamada.

### COMPROBACIÓN DEL ESTÁNDAR GSM EN LA PARTE RF.

Comenzaremos con la aplicación Agilent Spectrum Analyzer. Con ella se han tomado medidas en ambas bandas de: la potencia del canal, la potencia en canales adyacentes, el ancho de banda ocupado y la máscara del espectro de emisión.

Se montará el siguiente esquema según el manual del analizador en el cual, el generador de señales que aparece en el diagrama será sustituido por el equipo SDR que será el encargado de generar la señal GSM:




**52. MONTAJE PARA LAS MEDIDAS DEL CANAL GSM**

### ESTABILIDAD DEL RELOJ INTERNO DEL SDR

El equipo SDR utilizado dispone de una precisión en el reloj de 2.5ppm que, a la frecuencia de uso, unos 900MHZ aproximadamente, se corresponde a 2,25KHz de error. Este error no es apreciable para la realización y recepción de llamadas con los móviles, pero para el caso del analizador vectorial en modo de decodificador hay intervalos de tiempo que no es capaz de demodular bien la señal. Para mejorar la precisión, el equipo analizador dispone de una salida de 10Mhz estable que se conecta mediante un cable coaxial a la entrada de la señal de referencia del equipo SDR. El sistema OpenBTS dispone de un parámetro para indicarle que tome como referencia el reloj externo y no el interno. Las medidas anteriores se han tomado con el reloj externo configurado y conectado. Para el resto de test de operación con el móvil no ha sido necesario. A continuación se mostrarán las medidas realizadas.

Según el documento TS 45.010 del estándar GSM, se indica que se necesita una estabilidad del reloj superior a 0.05ppm (capítulo 5.1) pero para el caso de pico-bts, como el nuestro, esa condición se puede relajar hasta 0.1ppm.

### PARA LA BANDA DE 900MHZ

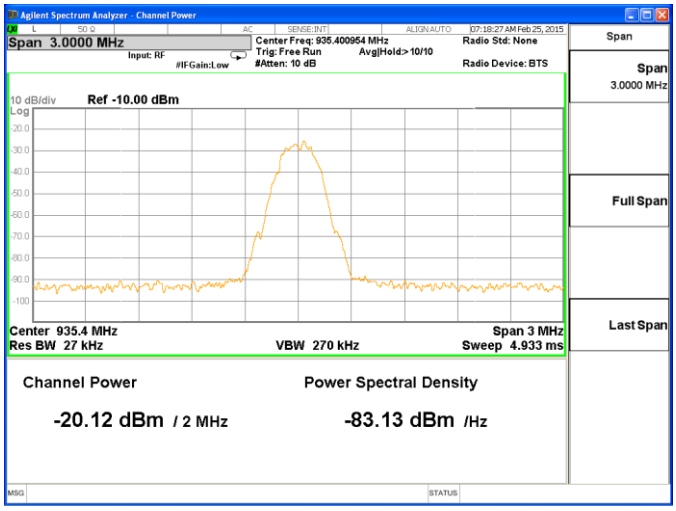
**Potencia del canal:** En nuestro caso el generador de señales es el propio equipo SDR funcionando con OpenBTS. Este test mide la potencia RF total presente en el canal GSM, los resultados se muestran tanto como potencia total en dBm como en densidad de potencia espectral dBm/Hz. Según el documento del estándar TS 45.005, en el apartado 4.1.2, se indica las diferentes clases de BTS en función de su potencia de salida. Para nuestro caso, como se puede ver en la medida siguiente, el test realizado se encuentra en el documento del estándar TS 51.021, apartado 6.3. En este test se describe la metodología a seguir para obtener la precisión de la potencia del emisor, es decir, que si desde el panel de control configuramos por ejemplo -20dBm, realmente estén saliendo por la boda de la antena esos -20dBm.

Literalmente dice el test:

*"The power shall be measured at each nominal power level as specified. As a minimum, one time slot shall be tested on each TRX. Any TRX which is a dedicated BCCH shall only be tested at highest static power step."*

*"La potencia debe medirse para cada nivel de potencia nominal tal y como se especifica. Como mínimo, se debe evaluar un time slot en cada TRX. Cualquier TRX dedicado a BCCH debe ser únicamente verificado a la mayor potencia de transmisión."*

Puesto que sólo disponemos de un TRX, con modulación GMSK, podemos utilizar la medida directa del analizador vectorial de un *timeslot*:




**53. POTENCIA DEL CANAL EN USO**

Gracias a este test podemos obtener la clasificación de nuestra BTS que con -20dBm, se clasifica según el estándar como una pico-BTS P1.

Colocado el transmisor a -20dBmW de potencia para evitar saturar el equipo de medida, podemos comprobar que la medida obtenida se aproxima a la teórica. Se encuentra dentro de los márgenes de tolerancia de la medida de +-2dB que indica el estándar. Internamente el analizador está configurado con otros 10dB de atenuación para protección, pero los compensa al mostrar los resultados y que sean transparentes al usuario.

**Potencia en canales adyacentes, ACP:** También se refiere a esta medida como ratio de potencia en canales adyacentes, ACPR de sus siglas en inglés o ratio de fuga en canales adyacentes, ACLR de sus siglas en inglés.

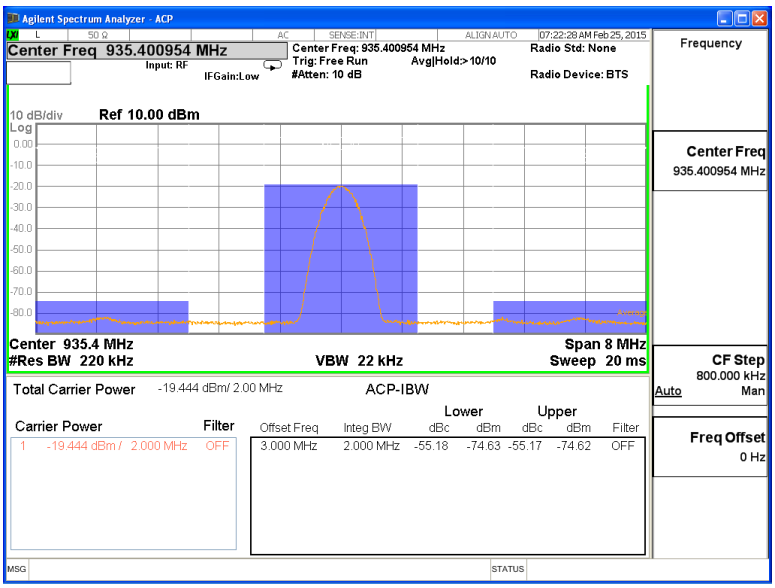
Este test se describe en el estándar TS 51.021, en el apartado 6.5. La finalidad del test es la de asegurar que para un TRX de una BTS, éste no interfiere ni introduce ruido por encima de un nivel máximo permitido.

El estándar indica que el equipo bajo test deberá ser puesto a prueba con un solo TRX activo en tres frecuencias (*Bottom, Middle, Top*).

- Colocar todos los *timeslot* a transmitir secuencias aleatorias. En nuestro caso emitimos en un solo TS, que por defecto si no hay comunicación transmite datos de forma aleatoria.
- Medir el nivel de potencia según el procedimiento anterior.

Hay más requisitos, pero no nos afectan porque es para BTS con más de un TRX y que transmiten más de un *timeslot*.

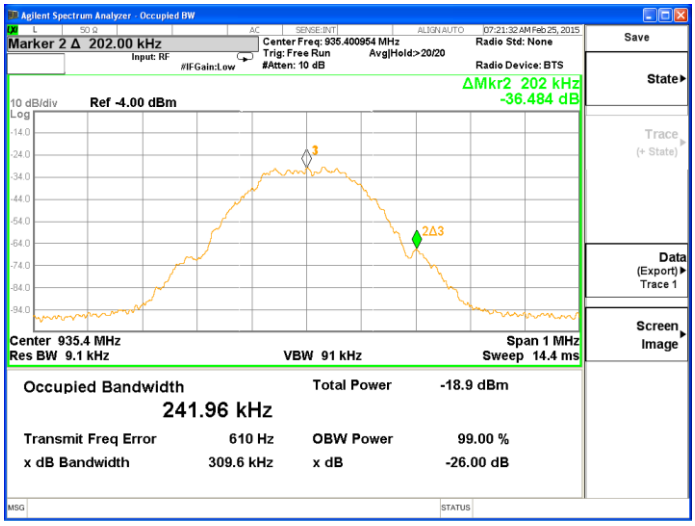
Tras tomar la medida, obtenemos los siguientes datos:




**54. POTENCIA EN CANALES ADYACENTES AL NUESTRO**

Según el estándar, puesto que transmitimos con <33dBm, el nivel de ruido deberá ser inferior a -65dBm, y como se puede observar en la gráfica de la medida, obtenemos un nivel de ruido de -74.65dBm para el caso de la frecuencia *Bottom*, y de -74.62dBm para el caso de la frecuencia *Top.* Por lo tanto esta BTS emite conforme al estándar. Traducido en una interferencia en bandas próximas casi nula y que es muy eficiente, ya que toda la potencia la emplea en la banda de interés.

**Ancho de banda ocupado:** Esta medida nos devuelve el ancho de banda ocupado por una estación GSM, calculando la potencia en toda la banda y calculando dónde está el 99% de esa potencia.




**55. ANCHO DE BANDA OCUPADO POR LA SEÑAL GSM**

En esta medida se pueden observar dos aspectos de la señal GMSK, por una parte la relación lóbulo principal a lóbulo secundario de 36.484dB y por otro lado el ancho de banda ocupado como se ha explicado con anterioridad, ocupa en el momento de la medida 241.96Khz y una potencia del canal de -18.9dbm.

Según el documento TS45.005 del estándar GSM, en el anexo A disponemos de la gráfica del espectro de la señal GSM y sus características:

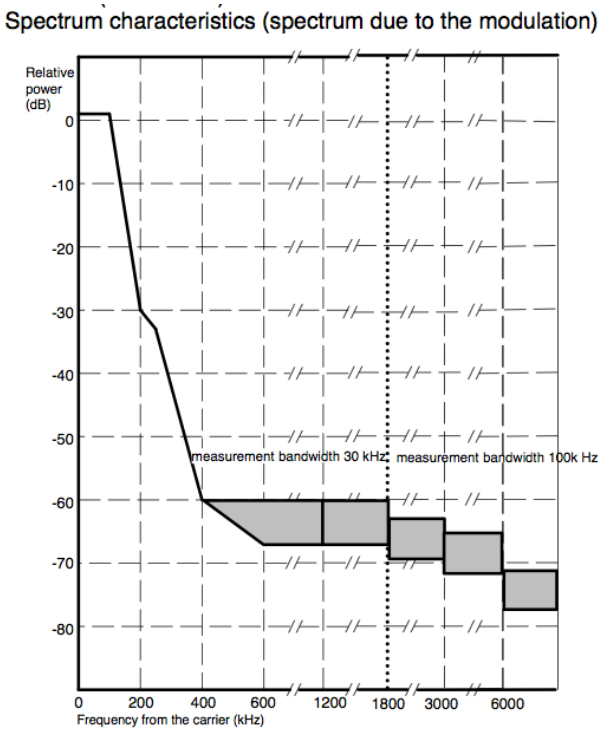



**Figure A.1a: GSM 400, GSM 900, GSM 850 and GSM 700 MS spectrum due to GMSK modulation**

**56. ESPECTRO GSM SEGÚN ESTÁNDAR**

Si comparamos ambos espectros, el del estándar, y el de nuestra medida, podemos ver que son muy parecidos, ya que a 200kHz del origen tenemos una caída de -30dBm según el estándar y de -36.484 según la medida (nótese que la medida es un promediado de 20 muestras y va cambiando con el

tiempo). El siguiente paso, a 400kHz del origen, según el estándar, la señal deberá estar a -60dBm, y según nuestra medida se observa que ha bajado otros 30dB respecto a la anterior. Con esto podemos decir que las características del espectro que genera nuestra BTS son conformes al estándar.

**Máscara del espectro de emisión:**

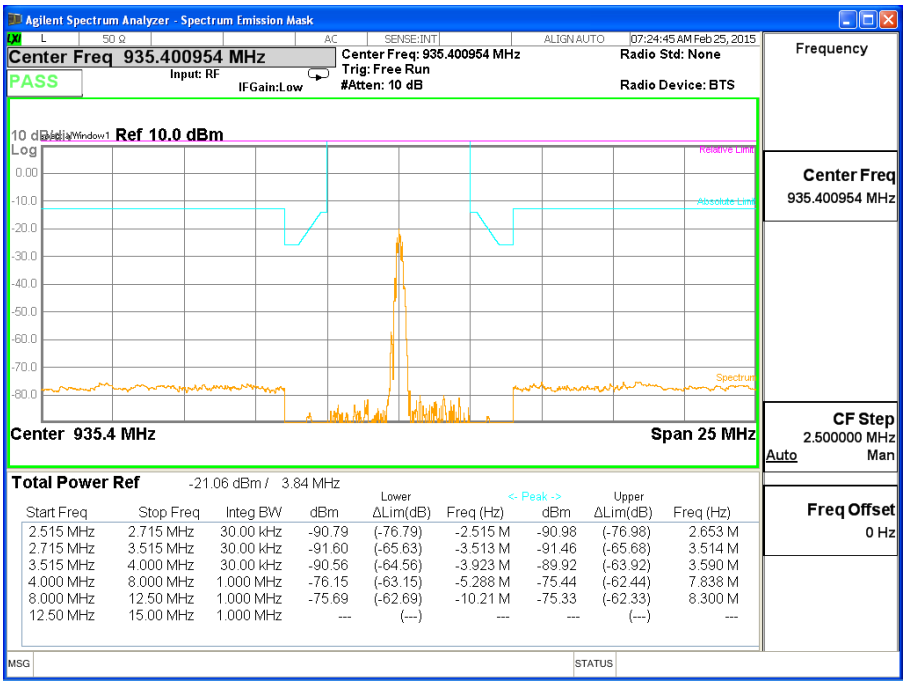
La ITU define la máscara del espectro de emisión como: *La máscara correspondiente a los casos críticos se aplica a los canales inferior y superior en la banda atribuida para proteger los servicios de radiocomunicaciones adyacentes, mientras que la correspondiente a los casos no críticos se aplica a la banda atribuida.*

Objetivo: Verificar si la potencia de cualquier emisión del transmisor no excede los niveles específicos para el ancho de banda del canal especificado.

| Spectrum emission limit (dBm)/ Channel bandwidth | | | | | | | |
|---|---|---|---|---|---|---|---|
| $\Delta f_{OOB}$ (MHz) | 1.4 MHz | 3.0 MHz | 5 MHz | 10 MHz | 15 MHz | 20 MHz | Measurement bandwidth |
| ± 0-1 | -10 | -13 | -15 | -18 | -20 | -21 | 30 kHz |
| ± 1-2.5 | -10 | -10 | -10 | -10 | -10 | -10 | 1 MHz |
| ± 2.5-2.8 | -25 | -10 | -10 | -10 | -10 | -10 | 1 MHz |
| ± 2.8-5 | | -10 | -10 | -10 | -10 | -10 | 1 MHz |
| ± 5-6 | | -25 | -13 | -13 | -13 | -13 | 1 MHz |
| ± 6-10 | | | -25 | -13 | -13 | -13 | 1 MHz |
| ± 10-15 | | | | -25 | -13 | -13 | 1 MHz |
| ± 15-20 | | | | | -25 | -13 | 1 MHz |
| ± 20-25 | | | | | | -25 | 1 MHz |

**57. NIVELES DE POTENCIA PARA LA MÁSCARA DE EMISIÓN**

Según los niveles que se indican en la tabla anterior, a continuación se muestra la medida realizada en la BTS en la banda GSM900:



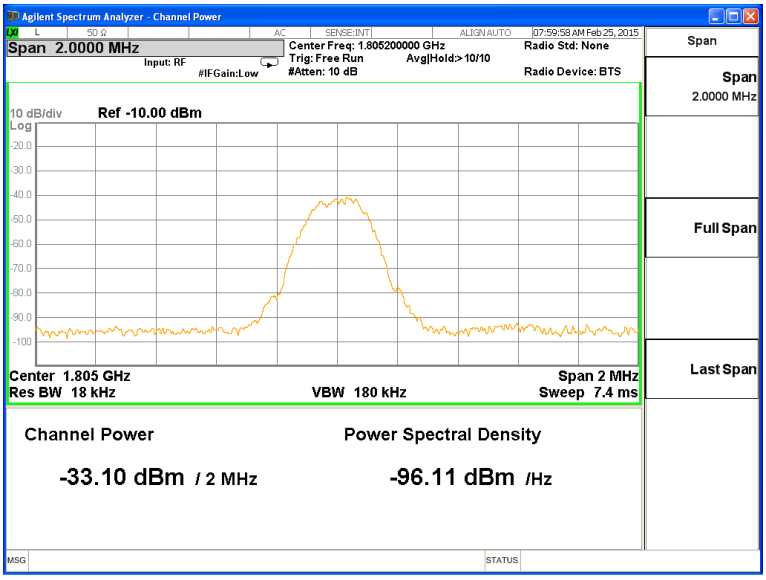

**58. MÁSCARA DEL ESPECTRO DE EMISIÓN**

Se puede observar cómo los niveles de potencia están muy por debajo de lo que indica la tabla 57 del estándar.

### PARA LA BANDA DE 1800MHZ

En este apartado se mostrarán los resultados obtenidos de realizar las mismas medidas que para la banda GSM, pero para la banda DCS.

**Potencia del canal:** La medida es la misma que para GSM, pero el equipo SDR tiene una limitación de potencia a frecuencias altas, por lo que en la configuración de OpenBTS se le baja la potencia de transmisión a -30dBm.

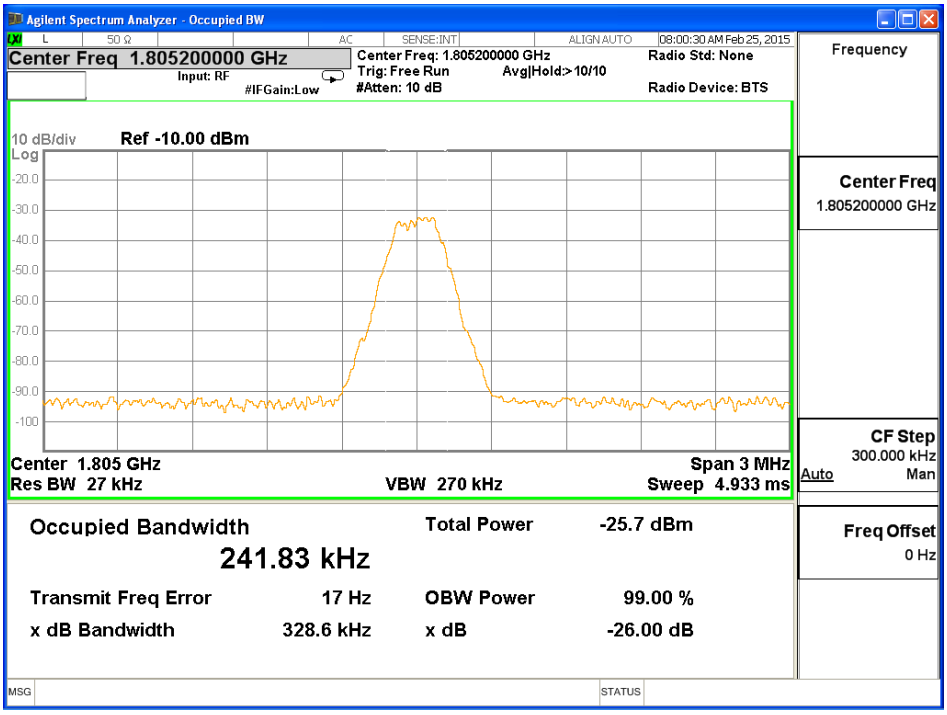



**59. POTENCIA DE TRANSMISIÓN EN DCS1800**

**Potencia en canales adyacentes:** La medida es la misma que para la banda GSM, pero al tener menor potencia de emisión se observa que la relación entre la potencia de canales adyacentes es algo mayor, de 44.8dB en este caso 7dB de diferencia.

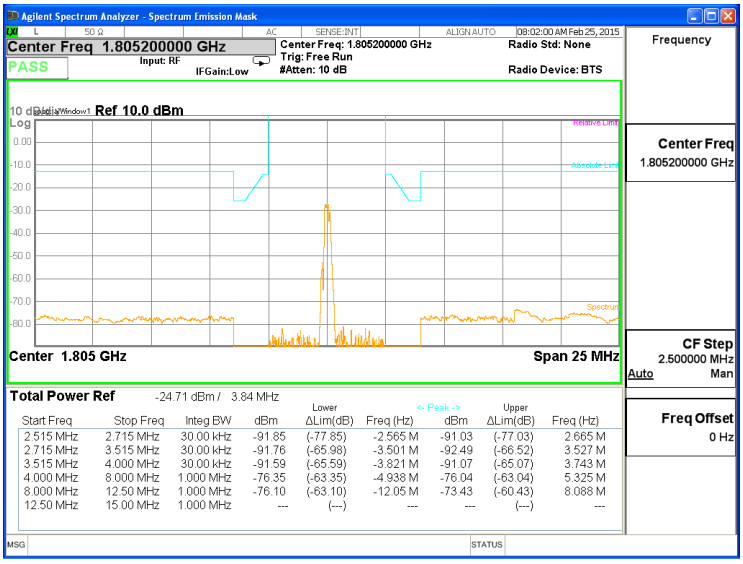
**60. POTENCIA EN CANALES ADYACENTES**

**Ancho de banda ocupado:** En este caso, la medida se aproxima bastante al caso de GSM900, 241.83Khz en DCS1800 frente los 241.96Khz de GSM900, 130Hz de diferencia en ancho de banda frente a los 7 dB de potencia.




**61. ANCHO DE BANDA OCUPADO**

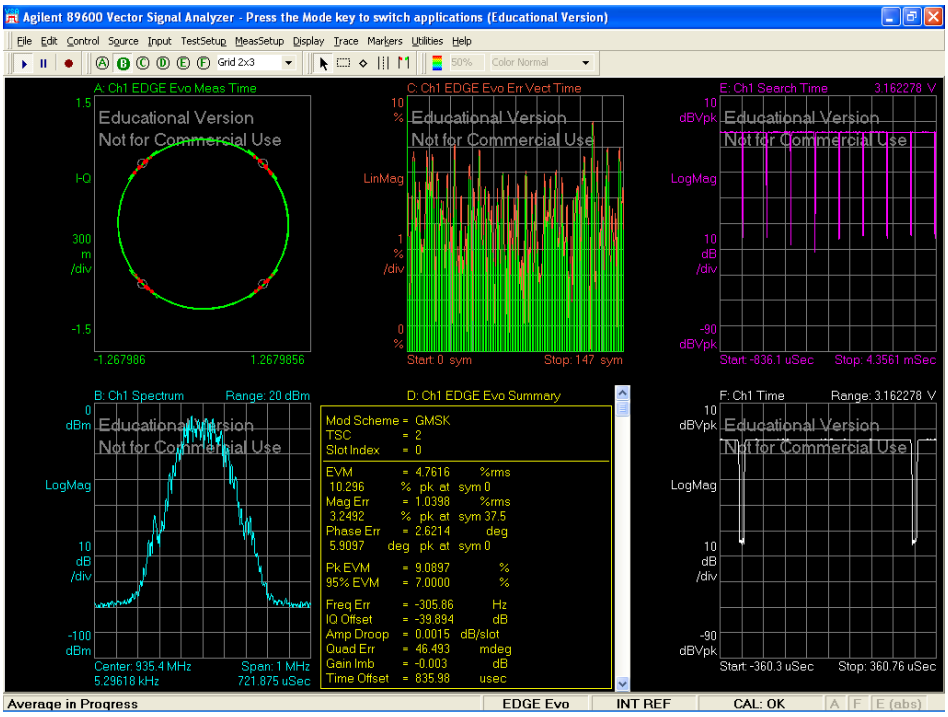
**Máscara del espectro de emisión:** La medida obtenida en este caso es idéntica al caso GSM900 ya que sólo tiene en cuenta el ancho de banda de la portadora, que en ambos casos es el mismo.




**62. MÁSCARA DEL ESPECTRO DE EMISIÓN**

MEDIDAS CON EL SOFTWARE VSA DEL ANALIZADOR VECTORIAL:

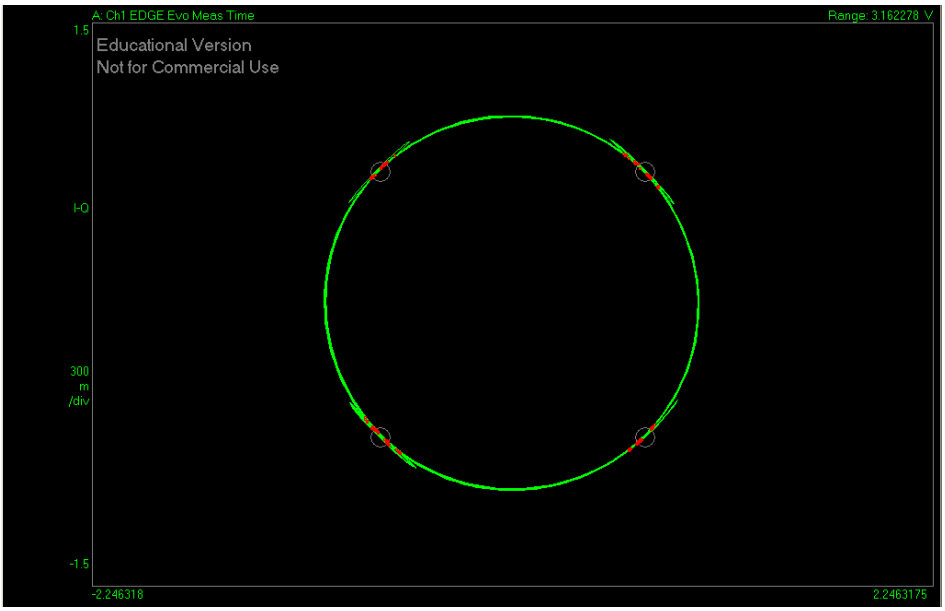
Como se ha comentado con anterioridad, el analizador vectorial dispone de otra aplicación para el análisis de señales digitales llamada VSA. Una vez configurada para obtener medidas de señales GSM, dentro del menú MeasSetup, tiene una apariencia como la siguiente figura:




**63. AGILENT 89600 VSA**

En esta aplicación podemos disponer en una misma pantalla multitud de información. Tenemos seis gráficas configurables, con las seis por defecto disponemos de:

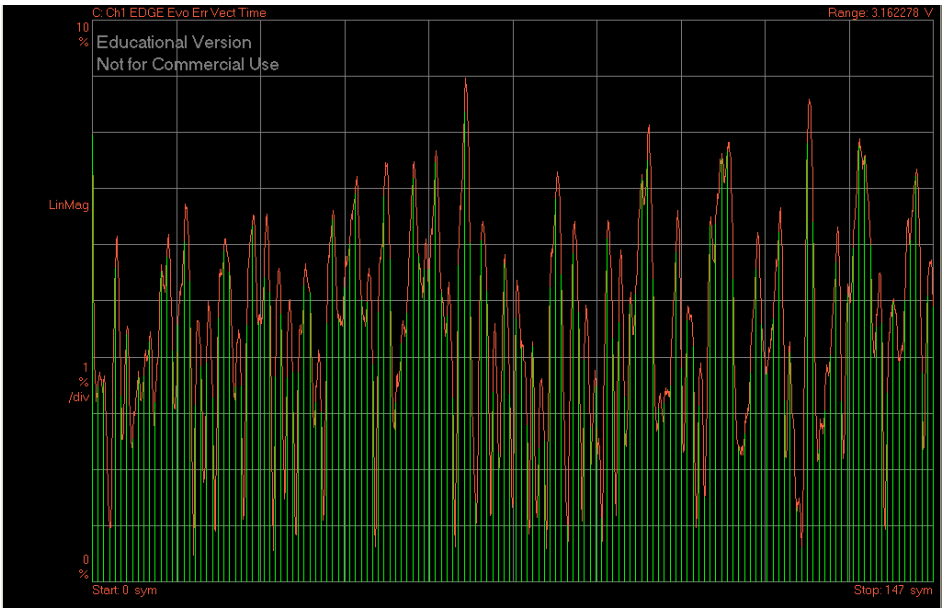
Gráfica de la constelación GMSK:




**64. CONSTELACIÓN GMSK EN VSA**

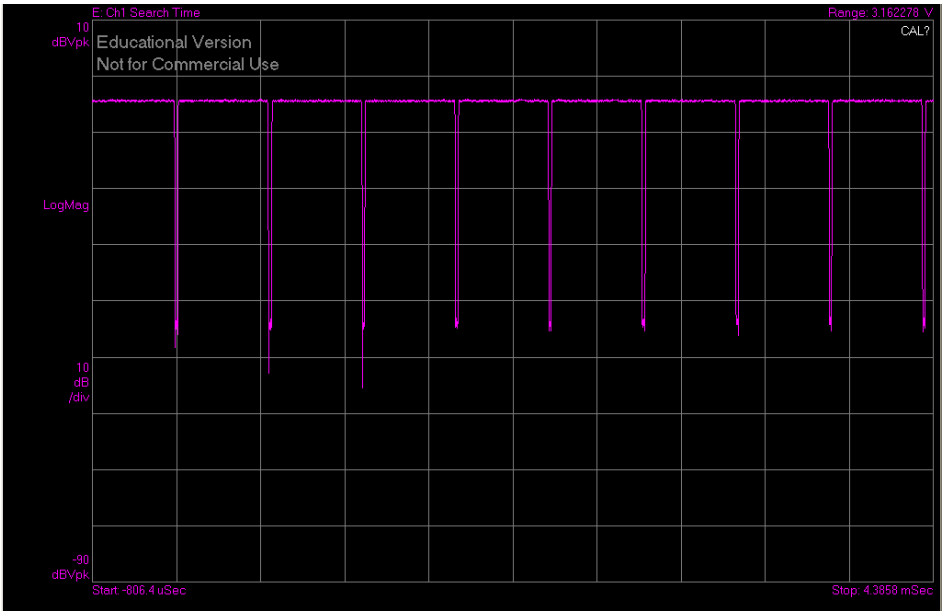
En el zoom realizado se puede observar donde realiza el muestreo de los cuatro símbolos, también se puede ver la interferencia intersimbólica propia de la modulación GMSK.

La siguiente gráfica que podemos ver es la correspondiente a la medida del error del vector del símbolo IQ, la siguiente imagen es un zoom a la misma, en la que se observa un error menor del 10% en todas las medidas:



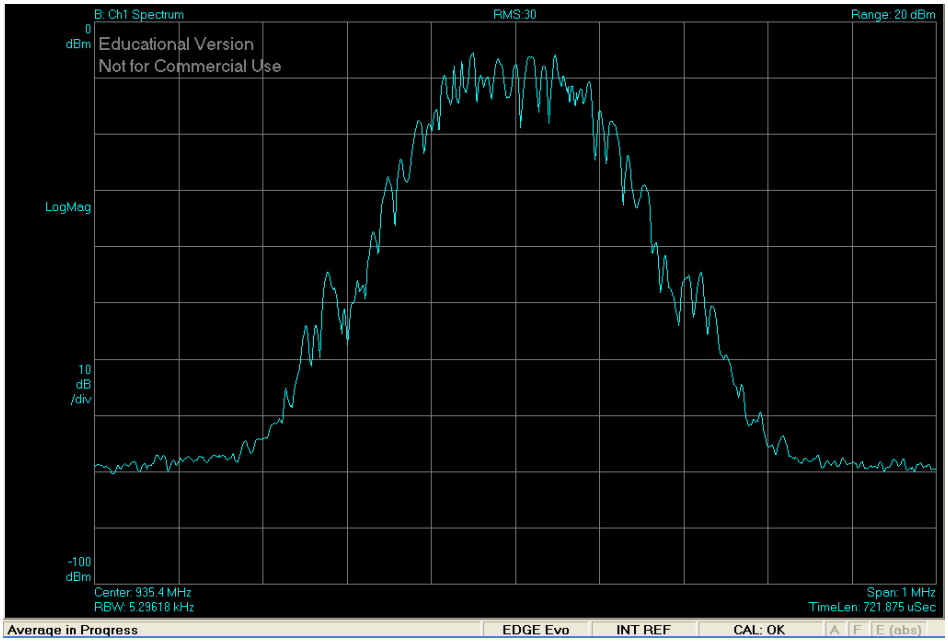

**65. ERROR DE VECTOR IQ EN CONSTELACIÓN**

La próxima medida mostrada en la pantalla principal corresponde a la visualización de un canal físico completo. Puesto que estamos midiendo el canal en el que transmite la BTS, aunque no esté ninguna comunicación en curso, transmite datos para aumentar la potencia media de transmisión:




**66. 8 TIME SLOTS DE C0**

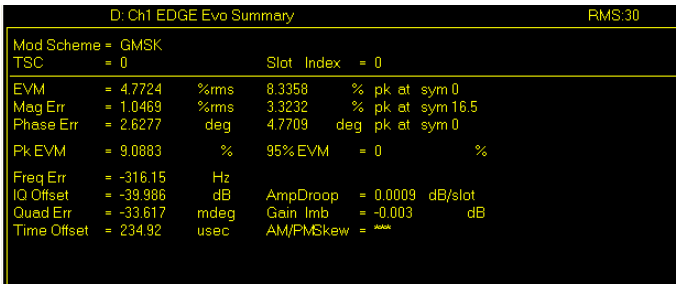
La medida siguiente se corresponde al espectro en tiempo real de la señal GMSK:




**67. ESPECTRO GSM**

Para poder visualizar un espectro que se aproxime a la señal teórica de GSM se ha configurado el software para que realice un promediado de 30 muestras de la señal.

Después, los datos que nos muestra el software, es un resumen de todas las medidas realizadas:

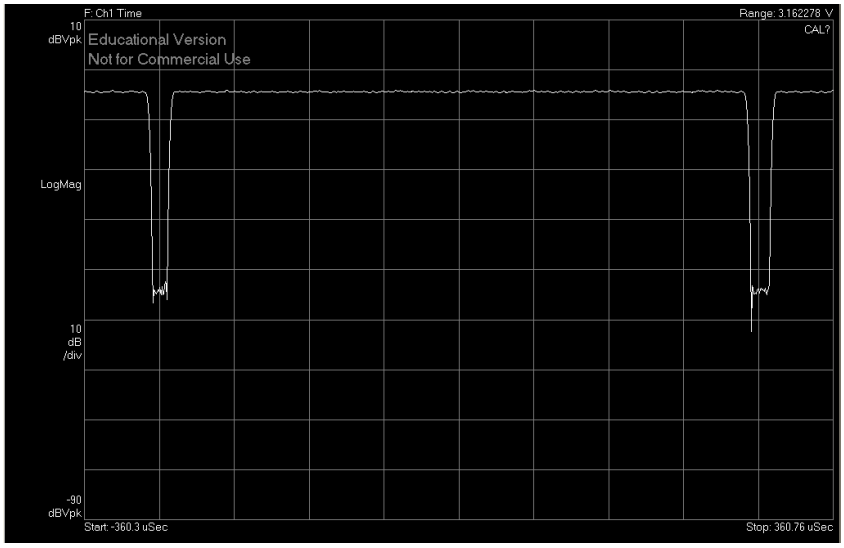



**68. RESUMEN MEDIDAS GSM EN VSA**

Al ver estos valores del resumen de medidas, según el estándar en el documento TS 51.021, en el apartado 6.2 dedicado a la precisión de la modulación del transmisor nos indica los valores máximos de error:

- Error de fase: 5 grados de pico. En nuestro caso obtenemos 2.6277 grados de error. Conforme.
- Error EVM de pico: 22% máximo según el estándar. 8.3358% de pico según nuestra medida. Conforme.

Y por último nos muestra una ráfaga o TS:



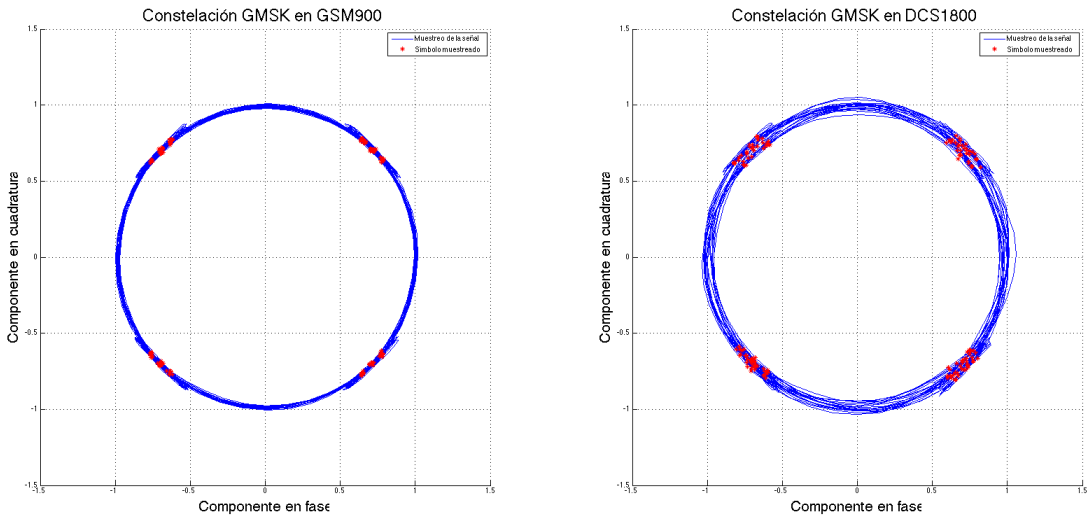

**69. RÁFAGA GSM**

En esta gráfica se puede ver que la duración de una ráfaga está en torno a 72us/div*8div=576us como máximo.

Ya se han visto las seis gráficas principales que dispone por defecto la aplicación. Una funcionalidad de la aplicación es la posibilidad de exportar los datos de cada gráfica por separado en diferentes formatos, entre ellos, uno de los más útiles para nosotros es el formato .mat de Matlab. Con esta información podemos realizar medidas y gráficas personalizadas.

Vista la posibilidad de mostrar los datos en Matlab, a continuación mostraremos las posibilidades de procesar esos datos en Matlab. Se han tomado medidas tanto en la banda GSM900 como DCS1800 y se podrán comparar de forma sencilla a partir de todos los datos exportados de las gráficas anteriores.

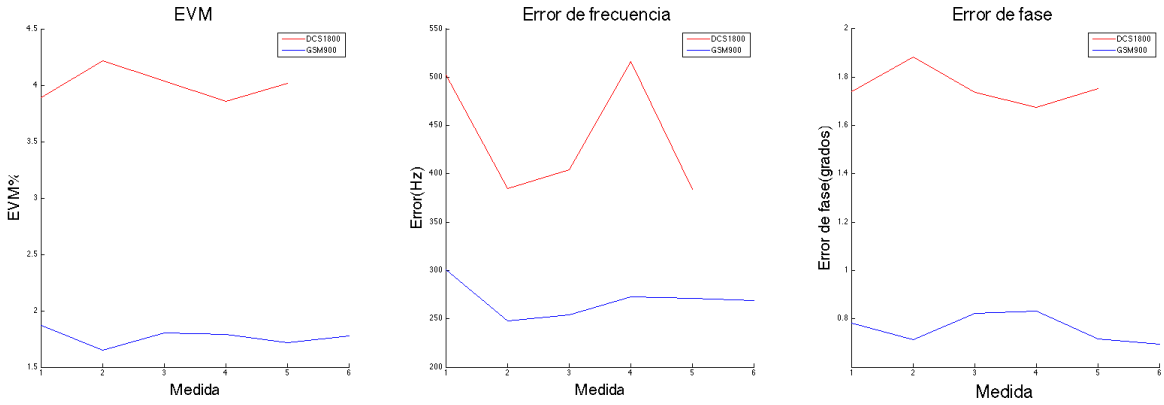
Comenzaremos con los datos IQ directos, con ellos podemos ver directamente la constelación de la modulación GMSK:




**70. CONSTELACIÓN GMSK EN GSM900 Y DCS1800**

Se puede observar cómo el error en frecuencia es mucho menor en la banda de 900Mhz ya que la línea está mucho más definida y los símbolos mucho más concentrados en sus posiciones teóricas. Por el contrario, en la banda de 1800Mhz el error en frecuencia es mayor, que se puede apreciar porque la línea es más difusa y los símbolos están más dispersos de la posición teórica. Este error se ha explicado al comienzo del capítulo, debido al error del reloj de 2.5ppm del equipo SDR.

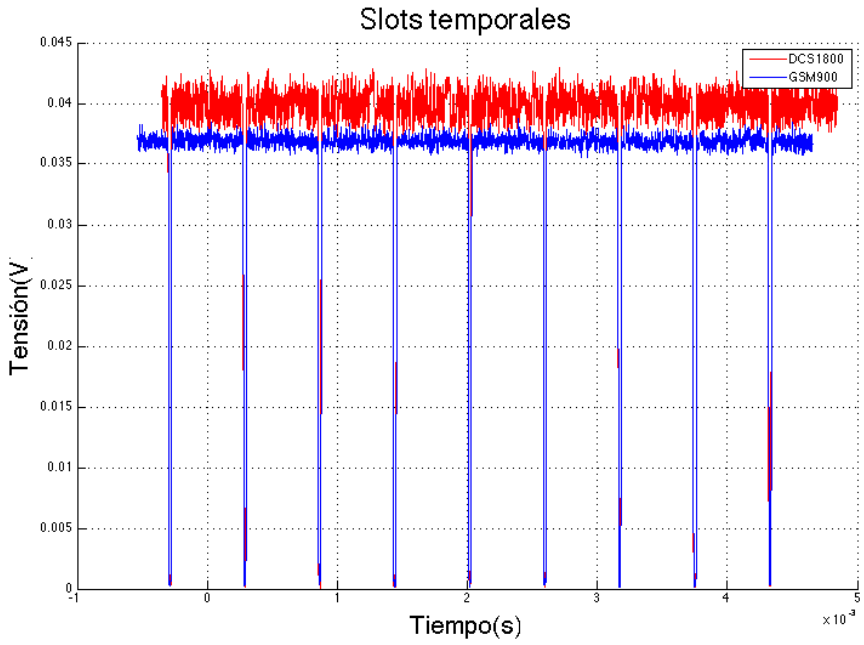
Dicho error también se ha medido con el equipo en diferentes medidas y mostrado en las gráficas siguientes:



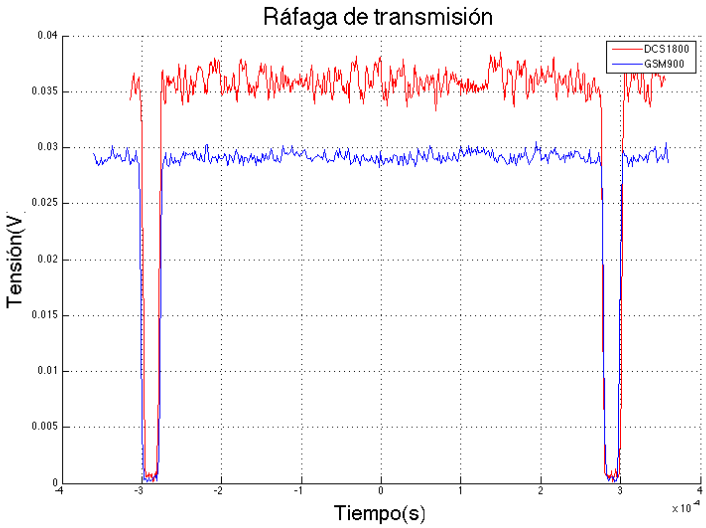

**71. ERRORES EN MEDIDAS**

En la gráfica anterior se pone de manifiesto lo comentado con anterioridad del error de frecuencia entre GSM900 y DCS1800 que produce el ensanchamiento de la gráfica de trayectoria del símbolo y el error de fase que produce la mayor dispersión en el muestro del símbolo transmitido.

También disponemos a nuestra disposición de los datos de los diferentes time slot como se puede observar en la siguiente muestra procesada con Matlab:



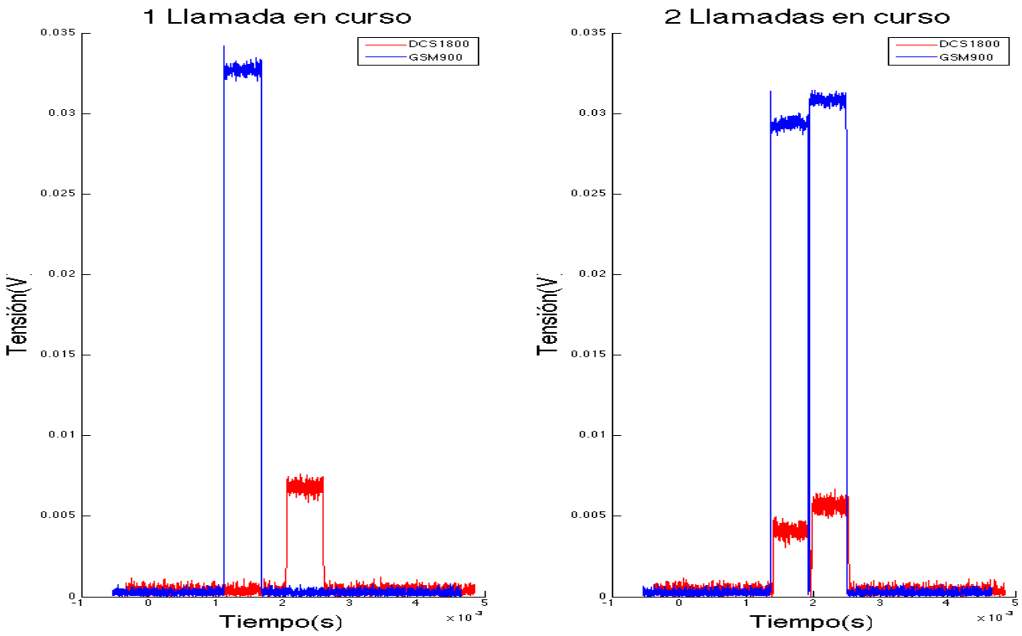

**72. SLOTS TEMPORALES DE UNA PORTADORA GSM**



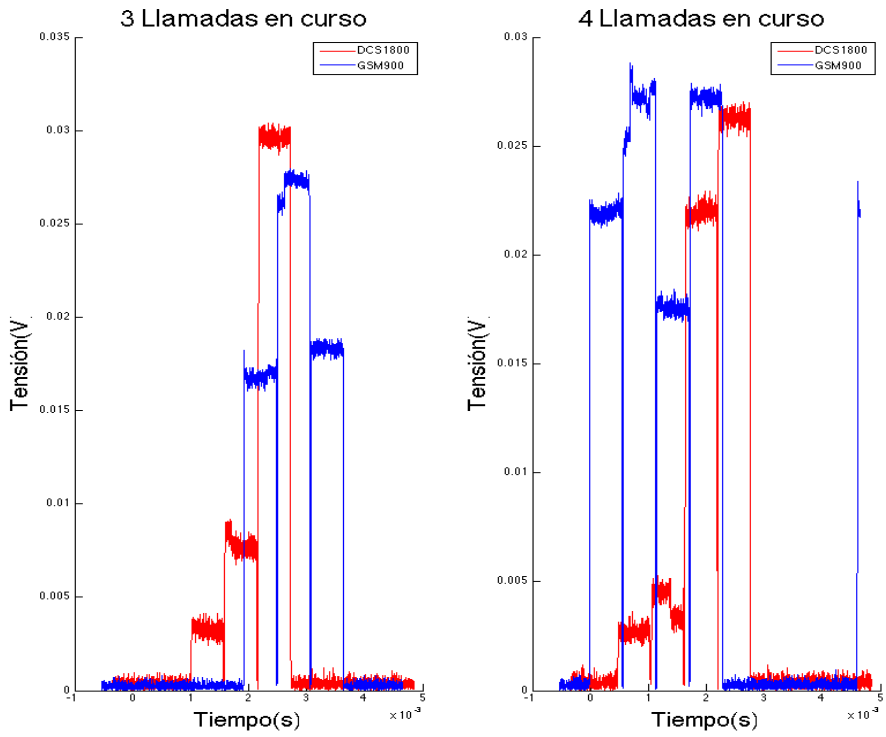

**73. RÁFAGAS EN UN SLOT TEMPORAL**

La gráfica de la izquierda es un canal de frecuencia con sus ocho time slot completos tanto en GSM900 como en DCS1800 podemos comprobar cómo la temporización en ambas bandas es idéntica. La gráfica de la derecha es un time slot concreto, una ráfaga en la banda de 900Mhz como en la de 1800Mhz, de nuevo se puede observar cómo la temporización es idéntica para las dos bandas.

Otra posibilidad del equipo es la de ver el canal ascendente directamente, pero para ello el montaje de test es diferente, ya que no podemos conectar el móvil directamente al analizador, para ello colocamos una antena GSM en la entrada del analizador para que reciba sin mucha degradación la señal del móvil. Tras cambiar la frecuencia de 934.2Mhz a 889.2Mhz=934.2Mhz-45Mhz y realizar diferentes llamadas, con diferentes móviles conectados a la BTS, podemos observar cómo éstas van ocupando diferentes time slot en los canales radio:




**74. SEÑAL TEMPORAL DEL ENLACE ASCENDENTE 1 Y 2 LLAMADAS SIMULTÁNEAS**




**75. SEÑAL TEMPORAL DEL ENLACE ASCENDENTE 3 Y 4 LLAMADAS SIMULTÁNEAS**

En la gráfica anterior también se pone de manifiesto cómo se reciben las llamadas con diferente potencia por la BTS y cómo van ocupando diferentes TS consecutivos con llamadas simultáneas. Los valores de potencia recibidos por el analizador vectorial son diferentes ya que cada MS está situado en una posición diferente.

Una vez visto el nivel radio de GSM, procederemos a estudiar el nivel de mensajes, para ello haremos uso de la herramienta Wireshark para capturar los paquetes generados tanto por la BTS como por el móvil.

## 4.3 ANÁLISIS DE LOS MENSAJES INTERCAMBIADOS ENTRE TODOS LOS SISTEMAS

En este epígrafe se van a mostrar los diferentes mensajes que genera tanto la BTS cómo el móvil El análisis de dichos mensajes se hace con la interfaz GSMTAP, que encapsula los mensajes GSM generados por la BTS sobre IP.

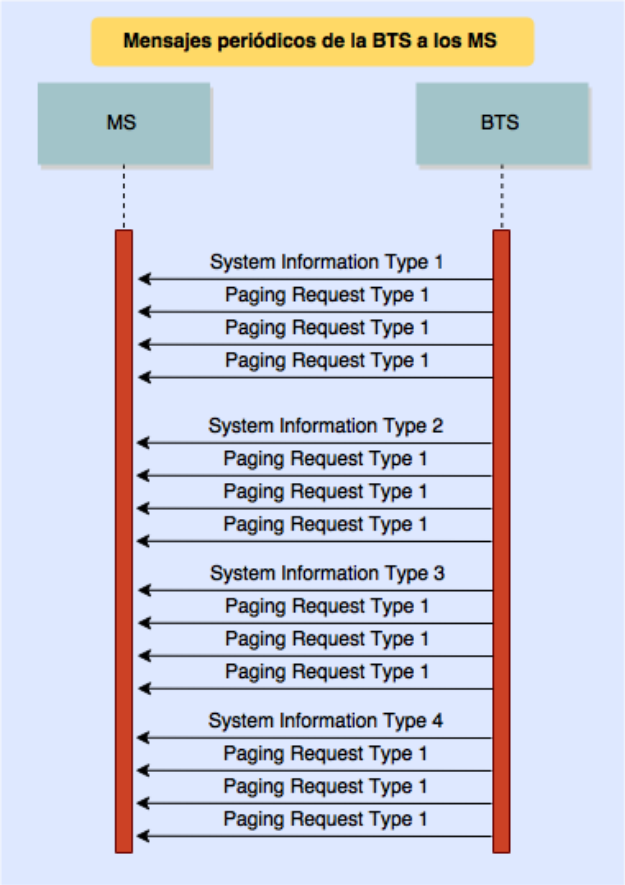
### 4.3.1 MENSAJES PERIÓDICOS DE LA BTS

La estación base comienza con la siguiente secuencia de mensajes:

| | | | | |
|---|---|---|---|---|
| 2578 18.818302 | 127.0.0.1 | 127.0.0.1 | GSMTAP | 87 (CCCH) (RR) System Information Type 1 |
| 2584 18.836832 | 127.0.0.1 | 127.0.0.1 | GSMTAP | 87 (CCCH) (RR) Paging Request Type 1 |
| 2591 18.865396 | 127.0.0.1 | 127.0.0.1 | GSMTAP | 87 (CCCH) (RR) Paging Request Type 1 |
| 2597 18.886696 | 127.0.0.1 | 127.0.0.1 | GSMTAP | 87 (CCCH) (RR) Paging Request Type 1 |
| 2607 19.054347 | 127.0.0.1 | 127.0.0.1 | GSMTAP | 87 (CCCH) (RR) System Information Type 2 |
| 2619 19.072045 | 127.0.0.1 | 127.0.0.1 | GSMTAP | 87 (CCCH) (RR) Paging Request Type 1 |
| 2626 19.100639 | 127.0.0.1 | 127.0.0.1 | GSMTAP | 87 (CCCH) (RR) Paging Request Type 1 |
| 2632 19.119994 | 127.0.0.1 | 127.0.0.1 | GSMTAP | 87 (CCCH) (RR) Paging Request Type 1 |
| 2642 19.290898 | 127.0.0.1 | 127.0.0.1 | GSMTAP | 87 (CCCH) (RR) System Information Type 3 |
| 2648 19.310205 | 127.0.0.1 | 127.0.0.1 | GSMTAP | 87 (CCCH) (RR) Paging Request Type 1 |
| 2655 19.338971 | 127.0.0.1 | 127.0.0.1 | GSMTAP | 87 (CCCH) (RR) Paging Request Type 1 |
| 2661 19.354214 | 127.0.0.1 | 127.0.0.1 | GSMTAP | 87 (CCCH) (RR) Paging Request Type 1 |
| 2671 19.527429 | 127.0.0.1 | 127.0.0.1 | GSMTAP | 87 (CCCH) (RR) System Information Type 4 |
| 2677 19.543915 | 127.0.0.1 | 127.0.0.1 | GSMTAP | 87 (CCCH) (RR) Paging Request Type 1 |
| 2684 19.572034 | 127.0.0.1 | 127.0.0.1 | GSMTAP | 87 (CCCH) (RR) Paging Request Type 1 |
| 2690 19.590988 | 127.0.0.1 | 127.0.0.1 | GSMTAP | 87 (CCCH) (RR) Paging Request Type 1 |

**76. MENSAJES PERIÓDICOS DE LA BTS**

Se puede observar que envían cuatro mensajes con información del sistema, que se verá con más detalle más adelante, y mensajes de *paging*.




**77. MENSAJES PERIÓDICOS DE LA BTS AL MS**

Detalle de los mensajes intercambiados:

```
▽ GSM TAP Header, ARFCN: 2 (Downlink), TS: 0, Channel: BCCH (0)
    Version: 2
    Header length: 16 bytes
    Payload Type: GSM Um (MS<->BTS) (1)
    Time Slot: 0
    ..00 0000 0000 0010 = ARFCN: 2
    .0.. .... .... .... = Uplink: 0
    Signal/Noise Ratio (dB): 0
    Signal Level (dBm): 0
    GSM Frame Number: 1099970
    Channel Type: BCCH (1)
    Antenna Number: 0
    Sub-Slot: 0
```

**78. CABECERA GSMTAP**

La capa superior de todos los mensajes GSM, corresponde a GSMTAP, en ella se puede ver que el tipo de carga es un mensajes GSM Um, que se va a transmitir por el canal ARFCN 2 *Downlink* BTS->MS, en el *TimeSlot* 0 y el tipo de canal lógico es BCCH.

```
▽ GSM CCCH - System Information Type 1
  ▽ L2 Pseudo Length
      0101 01.. = L2 Pseudo Length value: 21
  ▽ Protocol Discriminator: Radio Resources Management messages
      .... 0110 = Protocol discriminator: Radio Resources Management messages (0x06)
      0000 .... = Skip Indicator: No indication of selected PLMN (0)
    Message Type: System Information Type 1
  ▽ Cell Channel Description
      10.. 111. = Format Identifier: variable bit map (0x47)
      List of ARFCNs = 0
  ▽ RACH Control Parameters
      01.. .... = Max retrans: Maximum 2 retransmissions (1)
      ..11 10.. = Tx-integer: 32 slots used to spread transmission (14)
      .... ..0. = CELL_BARR_ACCESS: The cell is not barred (0)
      .... ...1 = RE: True
      0000 0100 0000 0000 = ACC: 0x0400
  ▷ SI 1 Rest Octets
```

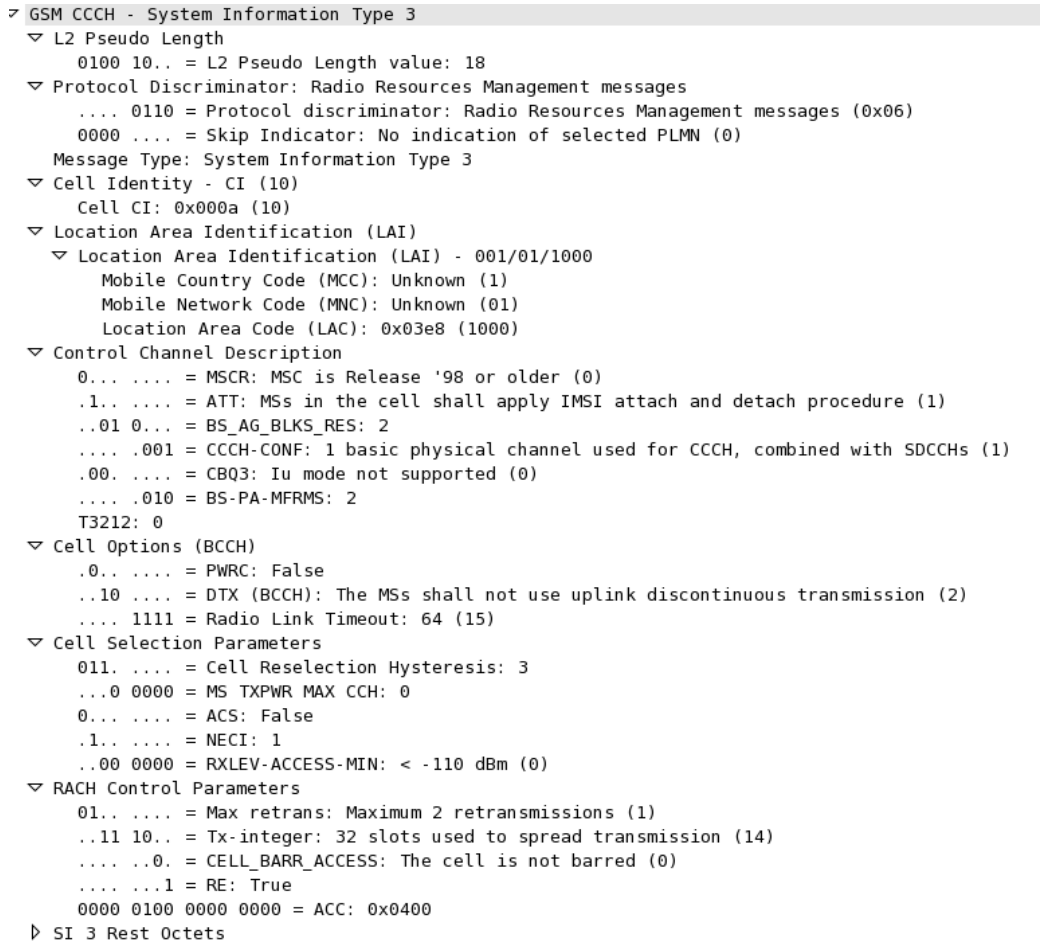
**79. MENSAJE SYSTEM INFORMATION TYPE 1**

La información más destacable del tipo 1 son los parámetros que le envía a los MS para cuándo éstos utilicen el canal RACH. El dato interesante es el número máximo de retransmisiones en caso de colisión al acceder al canal, que es de 2.

```
▽ GSM CCCH - System Information Type 2
  ▽ L2 Pseudo Length
      0101 10.. = L2 Pseudo Length value: 22
  ▽ Protocol Discriminator: Radio Resources Management messages
      .... 0110 = Protocol discriminator: Radio Resources Management messages (0x06)
      0000 .... = Skip Indicator: No indication of selected PLMN (0)
    Message Type: System Information Type 2
  ▽ Neighbour Cell Description - BCCH Frequency List
      ..0. .... = EXT-IND: The information element carries the complete BA (0)
      ...0 .... = BA-IND: 0
      10.. 111. = Format Identifier: variable bit map (0x47)
      List of ARFCNs = 2
  ▽ NCC Permitted
      0000 0001 = NCC Permitted: 0x01
  ▽ RACH Control Parameters
      01.. .... = Max retrans: Maximum 2 retransmissions (1)
      ..11 10.. = Tx-integer: 32 slots used to spread transmission (14)
      .... ..0. = CELL_BARR_ACCESS: The cell is not barred (0)
      .... ...1 = RE: True
      0000 0100 0000 0000 = ACC: 0x0400
```

**80. MENSAJE SYSTEM INFORMATION TYPE 2**

Este mensaje, el tipo 2, contiene gran parte de la información que contiene el tipo 1, pero en este caso le indica al móvil la información de las celdas vecinas, indicando las frecuencias de las mismas para que lo tenga en cuanta cuando necesite hacer un traspaso la llamada en curso.




**81. MENSAJE SYSTEM INFORMATION TYPE 3**

Este mensaje se transmite por el canal lógico CCCH y contiene, como se puede ver, mucha más información que los tipo 1 y 2. El primer dato que podemos observar es el identificador de la celda o CellId=10 (para entornos de test). Otra información que difunde la BTS es el LAI=001-01-1000 compuesta por el código del país MCC=001 (para entornos de test), el código del operador móvil MNC=01 (para entornos de test) y el código de área o LAC=1000 (entorno de test) No es una situación de campo por eso tiene esos valores asignados. Un ejemplo real podría ser: LAI = 214-07-360 que corresponde a un operador de España MCC=214, de Movistar MNC=07 y localizado en Santa Pola LAC=360. Seguimos con más datos que nos proporciona este mensaje, como por ejemplo, le indica al MS la necesidad de realizar el proceso de *IMSI attach* al acceder a la red y que cuando realice transmisión a la red, no utilice el modo discontinuo. Otro dato importante para el móvil a la hora de realizar un cambio de celda, es el valor de histéresis, ya que si se mueve por los límites de la celda estaría continuamente cambiando de una a otra, con este dato se controla dicha histéresis haciéndola mayor o menor en función de la necesidad del operador. En nuestro caso, como sólo disponemos de una celda, no es un dato crítico, pero si importante a la hora de realizar un despliegue con más celdas.

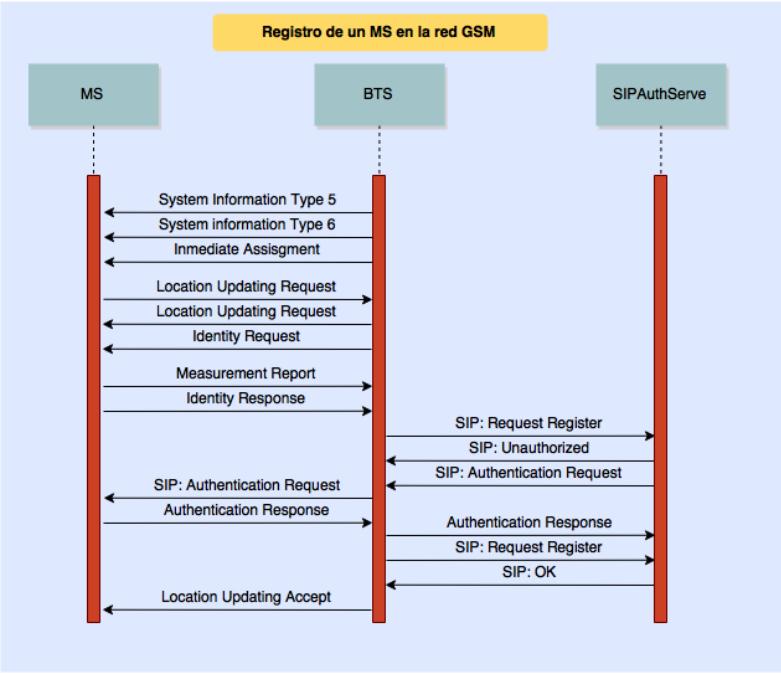
```
▽ GSM CCCH - System Information Type 4
  ▽ L2 Pseudo Length
      0011 00.. = L2 Pseudo Length value: 12
  ▽ Protocol Discriminator: Radio Resources Management messages
      .... 0110 = Protocol discriminator: Radio Resources Management messages (0x06)
      0000 .... = Skip Indicator: No indication of selected PLMN (0)
    Message Type: System Information Type 4
  ▽ Location Area Identification (LAI)
    ▽ Location Area Identification (LAI) - 001/01/1000
        Mobile Country Code (MCC): Unknown (1)
        Mobile Network Code (MNC): Unknown (01)
        Location Area Code (LAC): 0x03e8 (1000)
  ▽ Cell Selection Parameters
      011. .... = Cell Reselection Hysteresis: 3
      ...0 0000 = MS TXPWR MAX CCH: 0
      0... .... = ACS: False
      .1.. .... = NECI: 1
      ..00 0000 = RXLEV-ACCESS-MIN: < -110 dBm (0)
  ▽ RACH Control Parameters
      01.. .... = Max retrans: Maximum 2 retransmissions (1)
      ..11 10.. = Tx-integer: 32 slots used to spread transmission (14)
      .... ..0. = CELL_BARR_ACCESS: The cell is not barred (0)
      .... ...1 = RE: True
      0000 0100 0000 0000 = ACC: 0x0400
  ▷ SI 4 Rest Octets
```

**82. MENSAJE SYSTEM INFORMATION TYPE 4**

El mensaje tipo 4 contiene menor información que el tipo 3, pero los campos son los mismos. Lo único que no transmite es la información relativa a la descripción del canal de control común.

### 4.3.2 CONEXIÓN DE UN MÓVIL A LA RED GSM

Cuando aparece una comunicación por parte del móvil, la estación base transmite primero dos mensajes "*System Information Type 5*" y "*System Information Type 6*" y tras estos mensajes la asignación de canal de comunicaciones que deberá utilizar el móvil.




**83. MENSAJES INTERCAMBIADOS PARA EL REGISTRO DE UN MS EN LA RED GSM**

Al ser en este caso un encendido del teléfono, se realiza una actualización de la localización, para que se puedan dirigir las llamadas hacía él. Eso se puede observar en los siguientes mensajes una vez le han asignado el canal. Para poder realizar la actualización de la localización, el sistema le pide antes que se identifique el móvil, para saber si dispone de permiso o no para acceder a la red. La siguiente imagen muestra los mensajes comentados con anterioridad. Ahora pasaremos a detallar el contenido de dichos mensajes.

| | | | | | |
|---|---|---|---|---|---|
| 3260 | 23.715331 | 127.0.0.1 | 127.0.0.1 | LAPDm | 87 U, func=UI(DTAP) (RR) System Information Type 5 |
| 3266 | 23.733998 | 127.0.0.1 | 127.0.0.1 | LAPDm | 87 U, func=UI(DTAP) (RR) System Information Type 6 |
| 3279 | 23.779444 | 127.0.0.1 | 127.0.0.1 | GSMTAP | 87 (CCCH) (RR) Immediate Assignment |
| 3301 | 23.966892 | 127.0.0.1 | 127.0.0.1 | LAPDm | 81 U P, func=SABM(DTAP) (MM) Location Updating Request |
| 3303 | 23.969699 | 127.0.0.1 | 127.0.0.1 | LAPDm | 87 U F, func=UA(DTAP) (MM) Location Updating Request |
| 3309 | 23.971489 | 127.0.0.1 | 127.0.0.1 | LAPDm | 87 I, N(R)=0, N(S)=0(DTAP) (MM) Identity Request |

**84. MENSAJES DE CONEXIÓN A LA RED DE UN MÓVIL**

Comenzaremos con los mensajes de información del sistema 5 y 6:

```
▽ GSM TAP Header, ARFCN: 2 (Downlink), TS: 0, Channel: SACCH/4 (0)
    Version: 2
    Header length: 16 bytes
    Payload Type: GSM Um (MS<->BTS) (1)
    Time Slot: 0
    ..00 0000 0000 0010 = ARFCN: 2
    .0.. .... .... .... = Uplink: 0
    Signal/Noise Ratio (dB): 0
    Signal Level (dBm): 0
    GSM Frame Number: 1100724
    Channel Type: SACCH/4 (135)
    Antenna Number: 0
    Sub-Slot: 0
▽ SACCH L1 Header, Power Level: 16, Timing Advance: 0
    ...1 0000 = MS power level: 16
    .... .0.. = FPC: Not in use
    Actual Timing Advance: 0
▽ Link Access Procedure, Channel Dm (LAPDm)
  ▽ Address Field: 0x03
      .00. .... = LPD: Normal GSM (0)
      ...0 00.. = SAPI: RR/MM/CC (0)
      .... ..1. = C/R: 1
      .... ...1 = EA: Final octet (1)
  ▷ Control field: U, func=UI (0x03)
  ▷ Length Field: 0x49
▽ GSM A-I/F DTAP - System Information Type 5
  ▷ Protocol Discriminator: Radio Resources Management messages
    DTAP Radio Resources Management Message Type: System Information Type 5 (0x1d)
  ▽ Neighbour Cell Description - BCCH Frequency List
      ..0. .... = EXT-IND: The information element carries the complete BA (0)
      ...0 .... = BA-IND: 0
      10.. 111. = Format Identifier: variable bit map (0x47)
      List of ARFCNs = 2
```

**85. DATOS DE UN MENSAJE DE INFORMACIÓN DEL SISTEMA TIPO 5**

Este tipo de mensaje se envía por un canal SACCH como se puede ver en la cabecera GSM y contiene la información relativa a las celdas vecinas, mediante sus frecuencias BCCH, pero en este caso al ser una red con una sola BTS, dicha lista está sin datos.

```
GSM A-I/F DTAP - System Information Type 6
  Protocol Discriminator: Radio Resources Management messages
  DTAP Radio Resources Management Message Type: System Information Type 6 (0x1e)
  Cell Identity - CI (10)
      Cell CI: 0x000a (10)
  Location Area Identification (LAI)
    Location Area Identification (LAI) - 001/01/1000
        Mobile Country Code (MCC): Unknown (1)
        Mobile Network Code (MNC): Unknown (01)
        Location Area Code (LAC): 0x03e8 (1000)
  Cell Options (SACCH)
      .0.. .... = PWRC: False
      0.10 .... = DTX (SACCH): The MS shall not use uplink discontinuous transmission on a TCH-F. The MS shall not use uplink discontinuous transmission on TCH-H (2)
      .... 1111 = Radio Link Timeout: 64 (15)
  NCC Permitted
      0000 0001 = NCC Permitted: 0x01
```

**86. MENSAJE DE INFORMACIÓN DEL SISTEMA TIPO 6**

En el siguiente mensaje enviado por la BTS, el tipo 6, se transmite por el canal SACCH también tras el tipo 5. Este mensaje contiene información sobre la identidad de la celda (Cell Id) el área de localización de la misma (LAI=MNC+MNC+LAC) e información relativa a la celda, como el tiempo de desconexión (*timeout*=64) y lo más importante, indica al móvil que no está disponible la transmisión discontinua en los canales de tráfico TCH/F ni TCH/H por una limitación de OpenBTS. Esto último quiere decir que existe la posibilidad de que durante la ausencia de conversación en una llamada, el canal que está en uso se quedaría libre, pero esta funcionalidad no está implementada en OpenBTS.

```
GSM TAP Header, ARFCN: 2 (Downlink), TS: 0, Channel: CCCH (0)
    Version: 2
    Header length: 16 bytes
    Payload Type: GSM Um (MS<->BTS) (1)
    Time Slot: 0
    ..00 0000 0000 0010 = ARFCN: 2
    .0.. .... .... .... = Uplink: 0
    Signal/Noise Ratio (dB): 0
    Signal Level (dBm): 0
    GSM Frame Number: 1101055
    Channel Type: CCCH (2)
    Antenna Number: 0
    Sub-Slot: 0
```

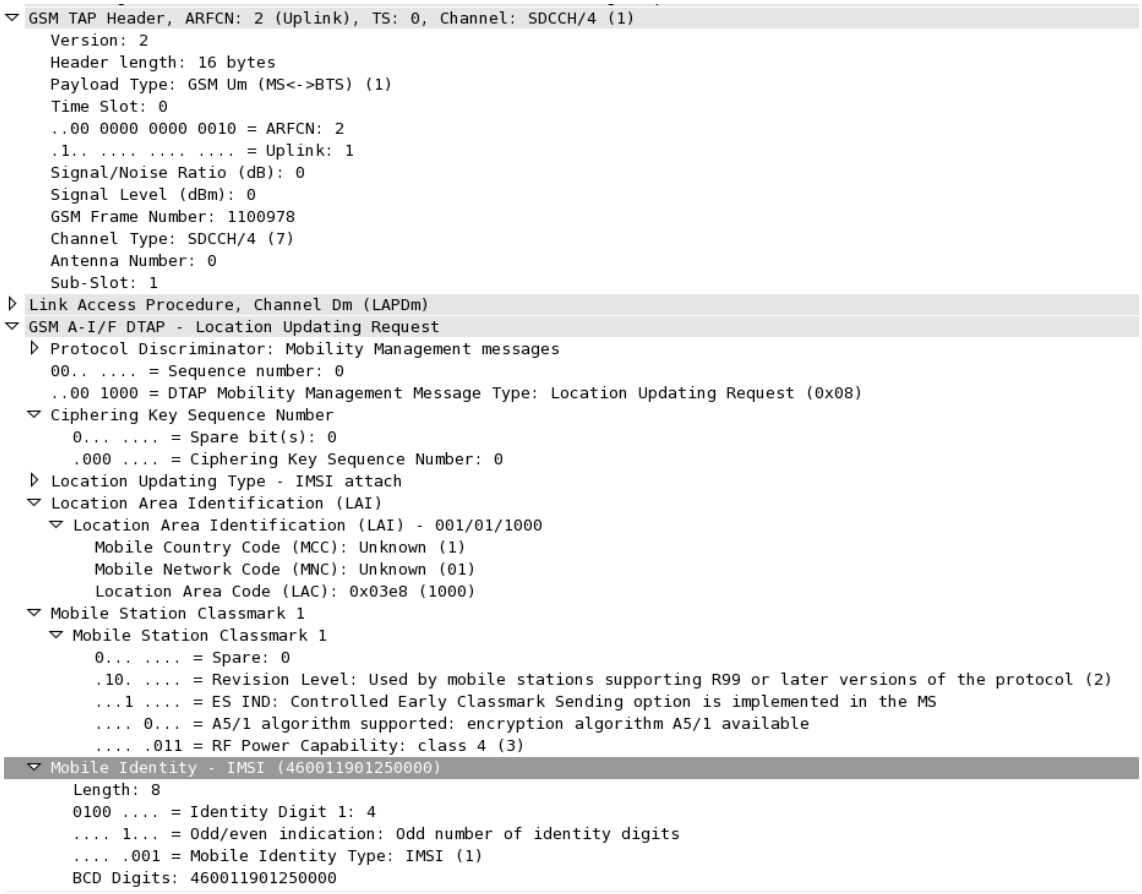
**87. CABECERA MENSAJE DE ASIGNACIÓN DE CANAL**

El siguiente mensaje enviado por la estación base es el de asignación de canal de tráfico al móvil. Se envía por un canal CCCH como se puede ver en la captura anterior.

```
GSM CCCH - Immediate Assignment
  L2 Pseudo Length
  Protocol Discriminator: Radio Resources Management messages
  Message Type: Immediate Assignment
  Page Mode
      .... 0000 = Page Mode: Normal paging (0)
  Dedicated mode or TBF
      0001 .... = Dedicated mode or TBF: This message assigns an uplink TBF or is the second message of two in a two-message assignment of an uplink or downlink TBF (1)
  Packet Channel Description
      0000 1... = Spare bits (ignored by receiver)
      .... .010 = Timeslot: 2
      010. .... = Training Sequence: 2
      ...0 .... = Hopping channel: No
      .... 00.. = Spare
      Single channel : ARFCN 2
  Request Reference
      Random Access Information (RA): 120
      1111 0... = T1': 30
      .... .010 100. .... = T3: 20
      ...0 1100 = T2: 12
      [RFN: 40208]
  Timing Advance
      Timing advance value: 0
  Mobile Allocation
      Length: 0
  IA Rest Octets
```

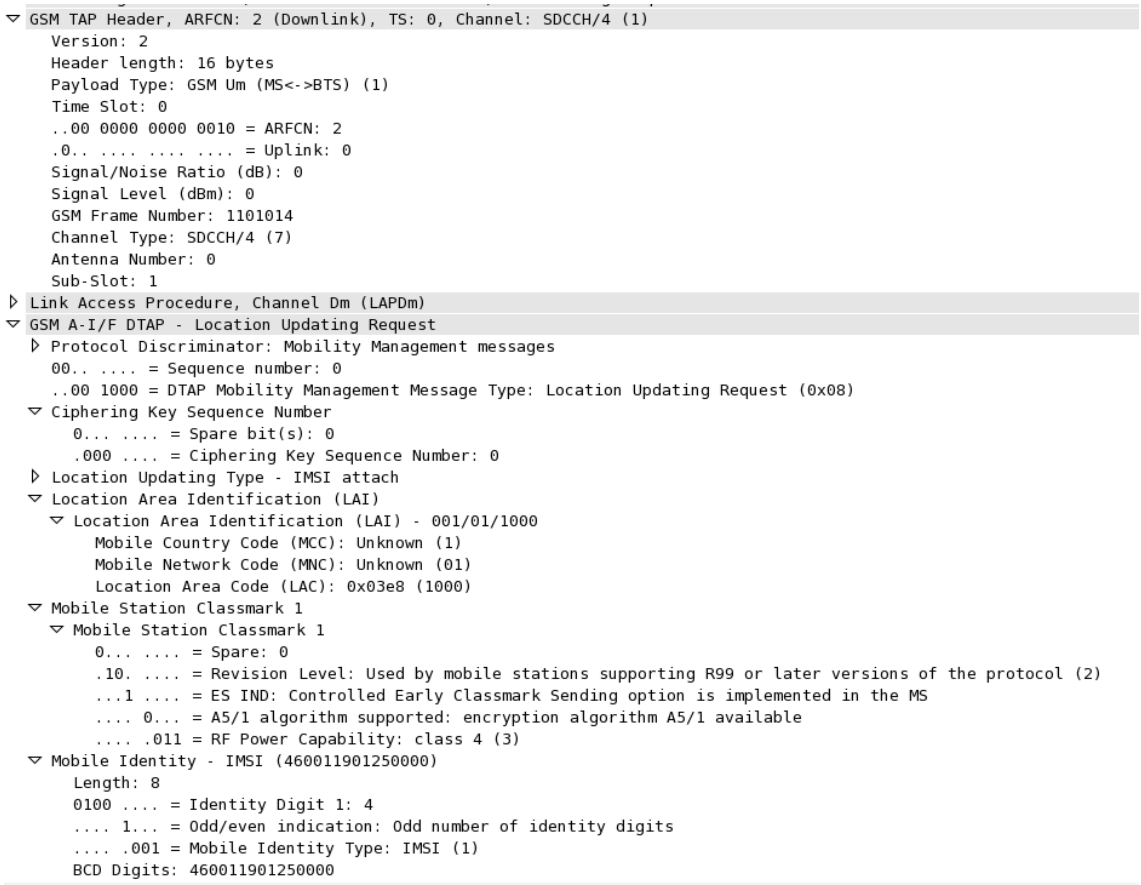
**88. MENSAJE DE ASIGNACIÓN DE CANAL DE TRÁFICO A UN MÓVIL**

Este es uno de los mensajes más importantes para el móvil, ya que con la información que contiene será capaz de comunicarse con la estación base. La información necesaria es el *timeslot* que deberá usar, en este caso es el número dos, la secuencia de entrenamiento que deberá transmitir para poder ecualizar el canal y mejorar la decodificación de los bits de datos, en este caso usará la secuencia número 2 que tanto emisor y receptor conocen. Y también le indica que no se va a hacer uso de la funcionalidad de salto en frecuencia porque no está implementada en OpenBTS.



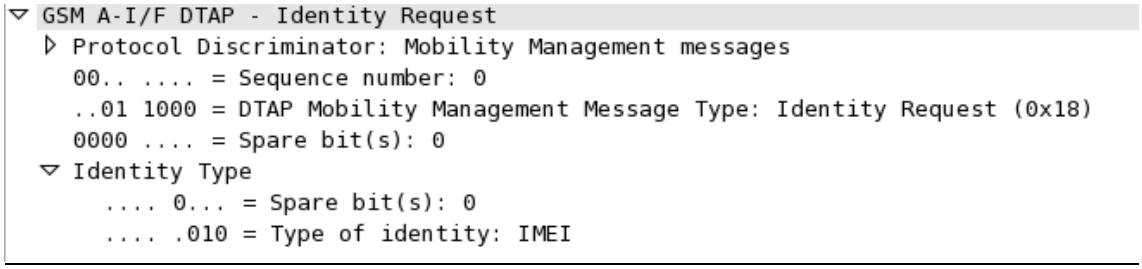

**89. MENSAJE DEL MÓVIL DE ACTUALIZACIÓN DE LOCALIZACIÓN**

Este mensaje es transmitido por el móvil a la estación base una vez que conoce el canal que le ha asignado con anterioridad para que se actualice su localización y pueda recibir llamadas. Se envía por un canal lógico SDCCH/4 como indica la cabecera GSM. Los datos que envía el móvil en este mensaje son numerosos como se puede ver en la captura anterior. Comenzaremos por los datos de cifrado de las comunicaciones, en el que indica el número de secuencia a utilizar para cifrar los datos transmitidos entre BTS y MS. Le indica que quiere realizar la acción de *IMSI attach* y la identificación del área en la que se encuentra el móvil (LAI). También se indica algunas características del móvil, como por ejemplo los algoritmos de cifrado soportados por el móvil, en este caso A5/1 y la capacidad de potencia del equipo, que en este caso es de clase 4. Otro dato muy importante que se puede observar en este mensaje es el identificador del abonado o IMSI que será el identificador a nivel global en GSM, en este caso es el 460011901250000.




**90. RESPUESTA A LA ACTUALIZACIÓN DE LOCALIZACIÓN POR PARTE DE LA BTS**

Una vez la BTS recibe el mensaje de petición de actualización de la posición por parte del móvil, ésta le responde con el mismo mensaje al móvil como se puede comprobar en la captura anterior.




**91. MENSAJE DE PETICIÓN DE IDENTIDAD**

Una vez realizada la petición de actualización de la posición por parte del móvil, la estación base le realiza una petición de identidad con un mensaje como el anterior, en el que le indica que la identidad se tomará en base al IMEI transmitido.

Una vez realizada la petición de que el dispositivo móvil se identifique, se realiza la autenticación en la centralita de llamadas Asterisk con el siguiente intercambio de mensajes:

```
LAPDm          81 U, func=UI(DTAP) (RR) Measurement Report
LAPDm          81 I, N(R)=1, N(S)=0(DTAP) (MM) Identity Response
SIP           711 Request: REGISTER sip:127.0.0.1 |
SIP           843 Status: 401 Unauthorized    (1 bindings) |
LAPDm          87 I, N(R)=1, N(S)=1(DTAP) (MM) Authentication Request
```

**92. INTENTO DE REGISTRO EN LA CENTRALITA DE LLAMADAS**

Comienza el MS con el envío de un informe de medidas de calidad del enlace radio a la BTS junto con la respuesta a la petición de identidad que se le requería con anterioridad. Una vez la BTS dispone de la identidad, ésta realiza una petición a la centralita de llamadas para registrar el móvil dentro de ella, aunque en este primer intento no se le autoriza dicho registro como se puede ver en el registro de mensajes ya que requiere antes de una autenticación del móvil en la centralita, aparte de la identificación en la BTS.

A continuación se detallarán los mensajes anteriores del proceso de intento de registro en la centralita Asterisk.

```
▽ GSM TAP Header, ARFCN: 2 (Uplink), TS: 0, Channel: SACCH/4 (1)
    Version: 2
    Header length: 16 bytes
    Payload Type: GSM Um (MS<->BTS) (1)
    Time Slot: 0
    ..00 0000 0000 0010 = ARFCN: 2
    .1.. .... .... .... = Uplink: 1
    Signal/Noise Ratio (dB): 0
    Signal Level (dBm): 0
    GSM Frame Number: 1101049
    Channel Type: SACCH/4 (135)
    Antenna Number: 0
    Sub-Slot: 1
▽ SACCH L1 Header, Power Level: 5, Timing Advance: 0
    ...0 0101 = MS power level: 5
    .... .1.. = FPC: In use
    Actual Timing Advance: 0
▷ Link Access Procedure, Channel Dm (LAPDm)
▽ GSM A-I/F DTAP - Measurement Report
  ▷ Protocol Discriminator: Radio Resources Management messages
    DTAP Radio Resources Management Message Type: Measurement Report (0x15)
  ▽ Measurement Results
      0... .... = BA-USED: 0
      .0.. .... = DTX-USED: DTX was not used
      ..11 1111 = RXLEV-FULL-SERVING-CELL: >= -48 dBm (63)
      0... .... = 3G-BA-USED: 0
      .1.. .... = MEAS-VALID: The measurement results are not valid
      RXLEV-SUB-SERVING-CELL: Unknown (127)
      .111 .... = RXQUAL-FULL-SERVING-CELL: BER > 12.8%, Mean value 18.10% (7)
      .... 111. = RXQUAL-SUB-SERVING-CELL: BER > 12.8%, Mean value 18.10% (7)
      .... ...0  00.. .... = NO-NCELL-M: No neighbour cell measurement result (0)
```

**93. INFORME DE MEDIDAS DE CALIDAD DEL ENLACE MS-BTS**

Este primer mensajes es el informe de la calidad del enlace radio, enviado por el móvil a la BTS, por el canal SACCH/4. Se puede observar información cómo el nivel de potencia del MS, el nivel de potencia de señal recibida por el móvil de la BTS, que es de -48dBm, indica también que no se está

utilizando tecnología 3G, otra indicación que efectúa es que los resultados finales de las medidas tomadas no son válidos ya que los siguientes datos sobrepasan el máximo permitido, es decir, la calidad de la recepción de señal por parte del móvil es menor a la permitida ya que recibe un BER medio del 18.10%, cuando el máximo permitido es del 12.8%. Esto no implica la pérdida del servicio, pero si cierta degradación de la calidad de las llamadas, por ello se le indica a la BTS que se ha sobrepasado el umbral de calidad de la señal recibida por el móvil.

```
▽ GSM A-I/F DTAP - Identity Response
  ▷ Protocol Discriminator: Mobility Management messages
    01.. .... = Sequence number: 1
    ..01 1001 = DTAP Mobility Management Message Type: Identity Response (0x19)
  ▽ Mobile Identity - IMEI (356603012547730)
      Length: 8
      0011 .... = Identity Digit 1: 3
      .... 1... = Odd/even indication: Odd number of identity digits
      .... .010 = Mobile Identity Type: IMEI (2)
      BCD Digits: 356603012547730
```

**94. RESPUESTA A LA PETICIÓN DE IDENTIDAD**

El siguiente mensaje, después del informe de calidad del enlace radio, es la respuesta a la petición de identificarse en la red, para ello envía el IMEI del móvil, ya que la BTS necesita el IMSI para registrar el móvil en la centralita y el IMEI para poder reconocer el móvil que contiene el IMSI dado.

```
▽ Session Initiation Protocol (REGISTER)
  ▷ Request-Line: REGISTER sip:127.0.0.1 SIP/2.0
  ▽ Message Header
    ▷ To:  <sip:IMSI460011901250000@127.0.0.1:5064>
    ▷ From:  <sip:IMSI460011901250000@127.0.0.1:5064>;tag=OBTSblujavjkpnxubnea
    ▷ Via: SIP/2.0/UDP 127.0.0.1:5062;branch=z9hG4bKOBTSnhadniqowtcgddbd
      Call-ID: 4571eb7feaa2fc9
    ▷ CSeq: 41145 REGISTER
    ▷ Contact: <sip:IMSI460011901250000@127.0.0.1:5062>;expires=5400
      Max-Forwards: 70
    ▷ P-Preferred-Identity: <sip:IMSI460011901250000@127.0.0.1>
    ▷ P-PHY-Info: OpenBTS; IMSI=no-MMUser TA=0 TE=-0.017578 UpRSSI=-16.000000 TxPwr=33 DnRSSIdBm=-48 time=1423132098.829
      P-Access-Network-Info: 3GPP-GERAN; cgi-3gpp=0010103e8000a
      User-Agent: OpenBTS 5.0-master Build Date 2015-01-12T18:50:06
      Content-Length: 0
```

**95. REGISTRO EN EL CORE DE LA RED**

El mensaje anterior, tras la identificación del MS en la BTS, corresponde a un mensaje entre la BTS y la centralita. LA BTS realiza un intento de registrar el IMSI dado con anterioridad en la centralita para que pueda cursar llamadas. Como estamos ante una centralita IP basada en el protocolo SIP, la BTS envía un mensaje tipo REGITER de SIP con el IMSI de la tarjeta SIM del móvil como identificador del abonado dentro de Asterisk.

```
▽ Session Initiation Protocol (401)
  ▽ Status-Line: SIP/2.0 401 Unauthorized
      Status-Code: 401
      [Resent Packet: False]
      [Request Frame: 3415]
      [Response Time (ms): 1]
  ▷ Message Header
```

**96. RESPUESTA AL INTENTO DE REGISTRO NO AUTORIZADO POR EL CORE**

En este primer intento de registrar el abonado, la centralita no le permite el acceso, ya que antes deberá de autenticarse, el mensaje anterior es la respuesta a ese intento de registro de la centralita a la BTS. Y por ello la BTS emite el mensaje siguiente al móvil, con la petición de autenticación.

```
▽ GSM A-I/F DTAP - Authentication Request
  ▷ Protocol Discriminator: Mobility Management messages
    00.. .... = Sequence number: 0
    ..01 0010 = DTAP Mobility Management Message Type: Authentication Request (0x12)
    0000 .... = Spare bit(s): 0
  ▽ Ciphering Key Sequence Number
      .... 0... = Spare bit(s): 0
      .... .000 = Ciphering Key Sequence Number: 0
  ▽ Authentication Parameter RAND - UMTS challenge or GSM challenge
      RAND value: d61b66b9b71808316eed3c4f5d252a10
```

**97. MENSAJE DE PETICIÓN DE AUTORIZACIÓN CIFRADA**

En el mensaje anterior de petición de autenticación, la BTS envía el test de cifrado, llamado *RAND value* y el número de secuencia del cifrado para que con el protocolo A5/1 el móvil responda al test y la BTS verifique que realmente es quien dice ser. Los siguientes mensajes ya sí se realiza el registro en Asterisk de forma correcta tras enviar el móvil la respuesta al test de cifrado anterior:

```
LAPDm          81 I, N(R)=2, N(S)=1(DTAP) (MM) Authentication Response
SIP           819 Request: REGISTER sip:127.0.0.1 |
SIP           911 Status: 200 OK    (1 bindings) |
```

**98. MENSAJES DE REGISTRO SATISFACTORIO EN ASTERISK**

A continuación veremos el detalle de los mensajes que finalmente consiguen registrar el móvil en la red VoIP de Asterisk.

```
▽ GSM A-I/F DTAP - Authentication Response
  ▷ Protocol Discriminator: Mobility Management messages
    00.. .... = Sequence number: 0
    ..01 0100 = DTAP Mobility Management Message Type: Authentication Response (0x14)
  ▽ Authentication Response Parameter
      SRES value: 33f373eb
```

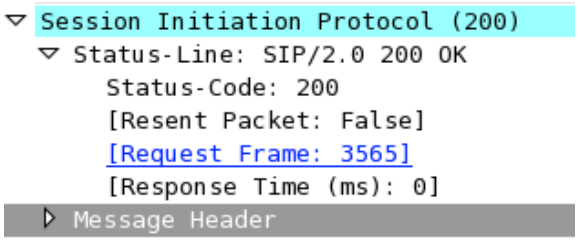
**99. MENSAJE DE RESPUESTA A LA PETICIÓN DE AUTORIZACIÓN CIFRADA**

Este mensaje lo envía el móvil con la respuesta al test de cifrado, dicha respuesta es *SRES value*. Que verifica la BTS y procede al registro en Asterisk con el siguiente mensaje:

```
▽ Session Initiation Protocol (REGISTER)
  ▷ Request-Line: REGISTER sip:127.0.0.1 SIP/2.0
  ▽ Message Header
    ▷ To:  <sip:IMSI460011901250000@127.0.0.1:5064>
    ▷ From:  <sip:IMSI460011901250000@127.0.0.1:5064>;tag=OBTSlnefqhxhkhtjsmxb
    ▷ Via: SIP/2.0/UDP 127.0.0.1:5062;branch=z9hG4bKOBTSsesuevgnpzlpfnph
      Call-ID: 4571eb7feaa2fc9
    ▷ CSeq: 41146 REGISTER
    ▷ Contact: <sip:IMSI460011901250000@127.0.0.1:5062>;expires=5400
    ▷ Authorization: Digest nonce="d61b66b9b71808316eed3c4f5d252a10", uri="460011901250000", response="33f373eb"
      Max-Forwards: 70
    ▷ P-Preferred-Identity: <sip:IMSI460011901250000@127.0.0.1>
    ▷ P-PHY-Info: OpenBTS; IMSI=no-MMUser TA=0 TE=-0.017090 UpRSSI=-16.000000 TxPwr=33 DnRSSIdBm=-48 time=1423132099.858
      P-Access-Network-Info: 3GPP-GERAN; cgi-3gpp=0010103e8000a
      User-Agent: OpenBTS 5.0-master Build Date 2015-01-12T18:50:06
```

**100. MENSAJE DE PETICIÓN DE REGISTRO EN ASTERISK**

En este mensaje se diferencia de la primera petición por la línea *Authorization*. Se presenta en esta línea el test enviado por la BTS, el IMSI del abonado y la respuesta del mismo.




**101. RESPUES DE REGISTRO ACEPTADO EN CENTRALITA**

Y una vez realizada la petición del registro con la autorización realizada por parte de BTS y MS, la centralita Asterisk, responde a la BTS indicando que ha registrado al móvil satisfactoriamente en la red. Una vez la BTS tiene conocimiento de esto, envía un mensaje al móvil, indicando que ya dispone de acceso a la red GSM con el siguiente mensaje:

```
LAPDm          87 I, N(R)=2, N(S)=3(DTAP) (MM) Location Updating Accept
```

**102. MENSAJE DE ACTUALIZACIÓN DE LA LOCALIZACIÓN ACEPTADO**

Y más en detalle:

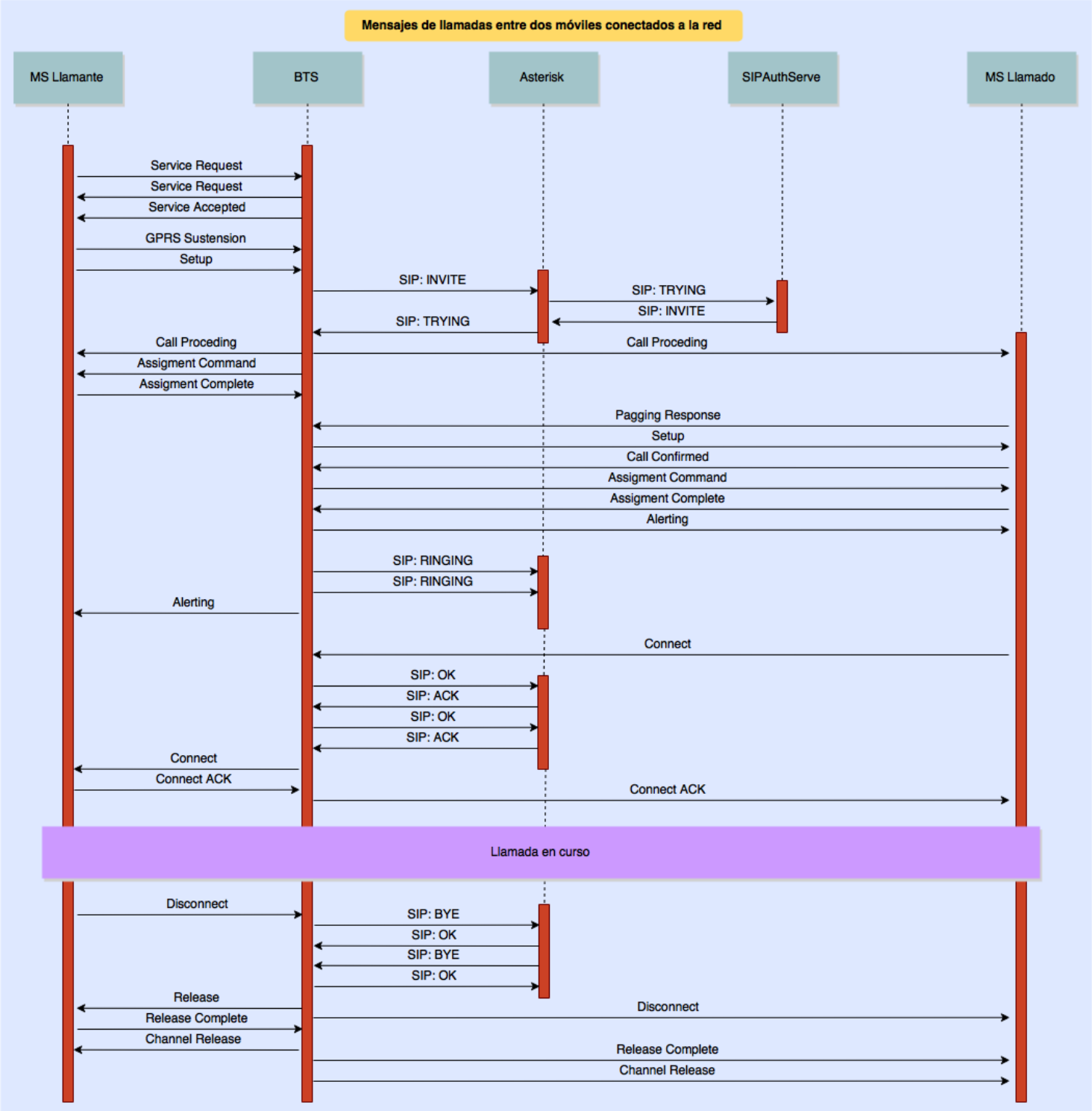
```
GSM A-I/F DTAP - Location Updating Accept
  Protocol Discriminator: Mobility Management messages
    00.. .... = Sequence number: 0
    ..00 0010 = DTAP Mobility Management Message Type: Location Updating Accept (0x02)
  Location Area Identification (LAI)
    Location Area Identification (LAI) - 001/01/1000
        Mobile Country Code (MCC): Unknown (1)
        Mobile Network Code (MNC): Unknown (01)
        Location Area Code (LAC): 0x03e8 (1000)
    Follow-on Proceed
```

**103. DETALLE DEL MENSAJE DE ACTUALIZACIÓN DE LA LOCALIZACIÓN ACEPTADA**

Como se puede ver en la captura anterior, el mensaje de confirmación contiene la confirmación de que está registrado en la red, y la identificación del área de localización, esto último se envía ya que se podría haber desplazado el móvil durante todo este proceso, por ejemplo durante un viaje en tren o coche el desplazamiento es muy rápido y en zonas muy pobladas las áreas de localización son más pequeñas para soportar más densidad de población.

### 4.3.3 REALIZACIÓN DE LLAMADAS ENTRE DOS MÓVILES CONECTADOS A OPENBTS

Una vez que el dispositivo móvil se ha podido conectar a la red GSM, analizaremos los mensajes intercambiados entre dos MS y la BTS ya que se va a realizar una llamada entre ellos.



Lo primero será la petición de un canal físico para poder enviar la señalización y la voz por parte del MS llamante, dichos mensajes entre MS llamante y BTS son los siguientes:

```
LAPDm          81 U P, func=SABM(DTAP) (MM) CM Service Request
LAPDm          87 U F, func=UA(DTAP) (MM) CM Service Request
LAPDm          87 I, N(R)=0, N(S)=0(DTAP) (MM) CM Service Accept
LAPDm          81 I, N(R)=0, N(S)=0(DTAP) (RR) GPRS Suspension Request
```

**104.MENSAJE DEL MÓVIL DE PETICIÓN DE ACCESO PARA LLAMADA**

Vamos a ver en detalle el contenido de estos mensajes para realizar la petición de un canal físico, ya que cuando el móvil llamado reciba la indicación de que tiene una llamada pendiente, intercambiará los mismos mensajes con la BTS para que se le asigne un canal físico para su parte de la comunicación.

El primer mensaje contiene la siguiente información:

```
▽ GSM A-I/F DTAP - CM Service Request
  ▷ Protocol Discriminator: Mobility Management messages
    00.. .... = Sequence number: 0
    ..10 0100 = DTAP Mobility Management Message Type: CM Service Request (0x24)
  ▽ Ciphering Key Sequence Number
      0... .... = Spare bit(s): 0
      .000 .... = Ciphering Key Sequence Number: 0
  ▽ CM Service Type
      .... 0001 = Service Type: (1) Mobile originating call establishment or packet mode connection establishment
  ▽ Mobile Station Classmark 2
      Length: 3
      0... .... = Spare: 0
      .10. .... = Revision Level: Used by mobile stations supporting R99 or later versions of the protocol (2)
      ...1 .... = ES IND: Controlled Early Classmark Sending option is implemented in the MS
      .... 0... = A5/1 algorithm supported: encryption algorithm A5/1 available
      .... .011 = RF Power Capability: class 4 (3)
      0... .... = Spare: 0
      .1.. .... = PS capability (pseudo-synchronization capability): PS capability present
      ..01 .... = SS Screening Indicator: Capability of handling of ellipsis notation and phase 2 error handling  (1)
      .... 1... = SM capability (MT SMS pt to pt capability): Mobile station supports mobile terminated point to point SMS
      .... .0.. = VBS notification reception: no VBS capability or no notifications wanted
      .... ..0. = VGCS notification reception: no VGCS capability or no notifications wanted
      .... ...1 = FC Frequency Capability: The MS does support the E-GSM or R-GSM
      1... .... = CM3: The MS supports options that are indicated in classmark 3 IE
      .0.. .... = Spare: 0
      ..0. .... = LCS VA capability (LCS value added location request notification capability): LCS value added location request notification capability not supported
      ...0 .... = UCS2 treatment: the ME has a preference for the default alphabet
      .... 0... = SoLSA: The ME does not support SoLSA
      .... .1.. = CMSP: CM Service Prompt: Network initiated MO CM connection request supported for at least one CM protocol
      .... ..1. = A5/3 algorithm supported: encryption algorithm A5/3 available
      .... ...0 = A5/2 algorithm supported: encryption algorithm A5/2 not available
  ▷ Mobile Identity - IMSI (460011901250000)
```

**105. MENSAJE DE PETICIÓN DE CANAL DE TRÁFICO**

La petición consta de: los datos necesarios para el cifrado de las comunicaciones; el tipo de petición, que en este caso es que el móvil va a realizar una llamada; datos del móvil que va a realizar la llamada, entre ellos, la potencia del móvil, el algoritmo de cifrado soportado, diferentes capacidades del móvil; y el identificador del abonado por su IMSI.

El mensaje de respuesta de la BTS al MS siguiente al anterior, es idéntico al mismo, por lo que no se pondrá una captura del mismo, ya que es idéntico, salvo por que va en dirección de la BTS al MS.

El siguiente mensaje sí es más interesante, ya que la BTS le indica al móvil que acepta su petición:

```
▽ GSM A-I/F DTAP - CM Service Accept
  ▷ Protocol Discriminator: Mobility Management messages
    00.. .... = Sequence number: 0
    ..10 0001 = DTAP Mobility Management Message Type: CM Service Accept (0x21)
```

**106. MENSAJE BTS-MS ACEPTANDO LA PETICIÓN DEL CANAL DE COMUNICACIONES**

El último mensaje que envía el móvil a la BTS es para que cierre la conexión debida al GPRS que pueda estar en curso, ya que no se soporta una comunicación simultánea entre una llamada GSM y navegar en internet por GPRS:

```
GSM A-I/F DTAP - GPRS Suspension Request
  Protocol Discriminator: Radio Resources Management messages
    DTAP Radio Resources Management Message Type: GPRS Suspension Request (0x34)
  TLLI - 0xc0040001
  Routing Area Identification - RAI: 1-1-1000-0
  Suspension Cause
      Suspension cause value: DTM not supported in the cell (6)
```

**107. MENSAJE DE CANCELACIÓN DE TRANSMISIÓN GPRS**

Una vez el móvil dispone de un canal físico de comunicaciones, éste envía un mensaje para preparar la BTS para la llamada entrante, para ello se intercambian los siguientes mensajes entre MS-BTS-Asterisk-SIPAuthserve.

```
LAPDm          81 I, N(R)=1, N(S)=2(DTAP) (CC) Setup
SIP/SDP       912 Request: INVITE sip:699666141@127.0.0.1:5060 |
SIP           505 Status: 100 Trying |
SIP/SDP       909 Request: INVITE sip:IMSI214190180026482@127.0.0.1:5062 |
SIP           474 Status: 100 Trying |
```

**108. MENSAJE DE INTENTO DE LLAMADA POR ASTERISK**

El primero de ellos es enviado por el móvil a la BTS, el siguiente lo envía la BTS a Asterisk para realizar la petición de llamada a la centralita, después Asterisk a SIPAuthserve con el primer mensaje *Trying* para conocer el IMSI del número llamado, y le responde SIPAuthserve con el usuario del llamante como IMSIXXXXXXXXX a Asterisk, Asterisk responde entonces a la BTS con el mensaje SIP *Trying*.

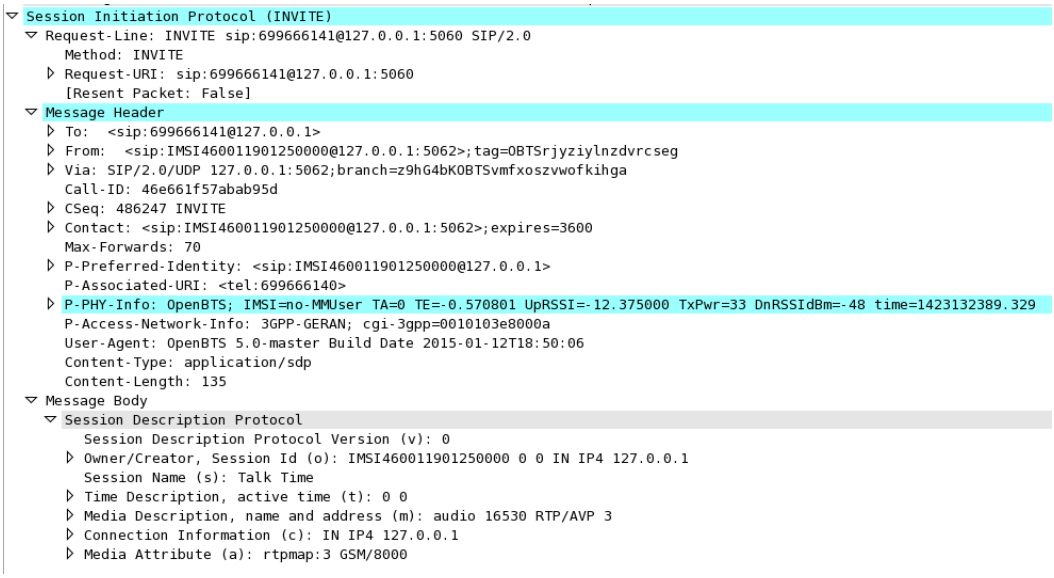
Se verán a continuación los detalles de los mensajes para aclarar este proceso:

```
GSM A-I/F DTAP - Setup
  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 version 1 than for half rate speech version 1)
  Called Party BCD Number - (699666141)
      Element ID: 0x5e
      Length: 6
      1... .... = Extension: No Extension
      .000 .... = Type of number: unknown (0x00)
      .... 0001 = Numbering plan identification: ISDN/Telephony Numbering (ITU-T Rec. E.164 / ITU-T Rec. E.163) (0x01)
      BCD Digits: 699666141
  Call Control Capabilities
      Element ID: 0x15
      Length: 2
      0000 .... = Maximum number of supported bearers: 1
      .... 0... = MCAT: The mobile station does not support Multimedia CAT
      .... .0.. = ENICM: The mobile station does not support the Enhanced Network-initiated In-Call Modification procedure
      .... ..1. = PCP: the mobile station supports the Prolonged Clearing Procedure
      .... ...1 = DTMF: the mobile station supports DTMF as specified in subclause 5.5.7 of TS 24.008
      0100 .... = Spare bit(s): 4
      .... 0101 = Maximum number of speech bearers: 5
    Extraneous Data
```

**109. MENSAJE DE MS-BTS PARA PREPARAR LA LLAMADA**

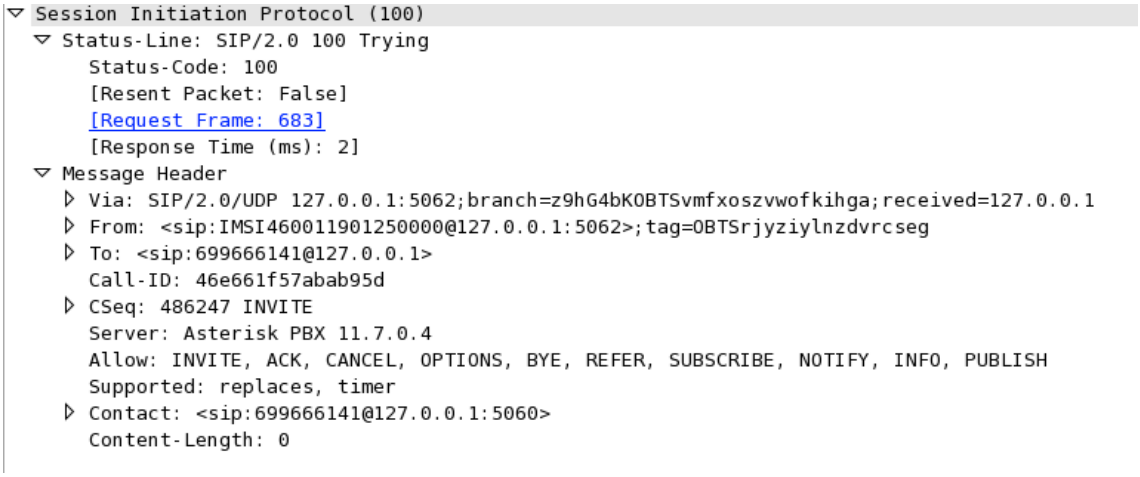
En este mensaje el móvil le indica a la BTS entre otros datos, los códec que soporta para realizar la llamada y el número de teléfono del móvil llamado 699666141.

El siguiente mensaje, de la BTS a Asterisk contiene la siguiente información:




**110. MENSAJE SIP PARA REALIZAR LA LLAMADA DE LA BTS A ASTERISK**

La BTS indica en el mensaje SIP el origen de la llamada por medio del usuario IMSI460011901250000 y el destino como un número de teléfono 699666141. Incluye más información sobre los códec de audio soportados. El siguiente mensaje lo realiza Asterisk al servidor de usuarios, SIPAuthServe, para obtener el usuario tipo IMSIXXXXXXXXXXX al que le corresponde el número de teléfono 699666141.




**111. MENSAJE DE ASTERISK A SIPAUTHSERVE PARA OBTENER EL IMSI DE UN NÚMERO**

A ese mensaje anterior el servidor de usuarios, SIPAuthserve, responde a Asterisk con el usuario IMSI para poder continuar con el proceso de llamada:

```
▽ Session Initiation Protocol (INVITE)
  ▽ Request-Line: INVITE sip:IMSI214190180026482@127.0.0.1:5062 SIP/2.0
      Method: INVITE
    ▷ Request-URI: sip:IMSI214190180026482@127.0.0.1:5062
      [Resent Packet: False]
  ▽ Message Header
    ▷ Via: SIP/2.0/UDP 127.0.0.1:5060;branch=z9hG4bK669a7221
      Max-Forwards: 70
    ▷ From: "699666140" <sip:699666140@127.0.0.1>;tag=as53da5cdb
    ▷ To: <sip:IMSI214190180026482@127.0.0.1:5062>
    ▷ Contact: <sip:699666140@127.0.0.1:5060>
      Call-ID: 5a360f7b6321ca32487c9df415be5e14@127.0.0.1:5060
    ▷ CSeq: 102 INVITE
      User-Agent: Asterisk PBX 11.7.0.4
      Date: Thu, 05 Feb 2015 10:33:10 GMT
      Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO, PUBLISH
      Supported: replaces, timer
      Content-Type: application/sdp
      Content-Length: 278
  ▽ Message Body
    ▽ Session Description Protocol
        Session Description Protocol Version (v): 0
      ▷ Owner/Creator, Session Id (o): root 1673567206 1673567206 IN IP4 127.0.0.1
        Session Name (s): Asterisk PBX 11.7.0.4
      ▷ Connection Information (c): IN IP4 127.0.0.1
      ▷ Time Description, active time (t): 0 0
      ▷ Media Description, name and address (m): audio 20852 RTP/AVP 3 0 8 101
      ▷ Media Attribute (a): rtpmap:3 GSM/8000
      ▷ Media Attribute (a): rtpmap:0 PCMU/8000
      ▷ Media Attribute (a): rtpmap:8 PCMA/8000
      ▷ Media Attribute (a): rtpmap:101 telephone-event/8000
      ▷ Media Attribute (a): fmtp:101 0-16
      ▷ Media Attribute (a): ptime:20
        Media Attribute (a): sendrecv
```

**112. MENSAJE DE RESPUESTA DE LA PETICIÓN DEL IMSI DE UN NÚMERO**

En el campo del mensaje "*From:*", indica el teléfono llamante 699666140, y el destino de la petición se indica el usuario IMSI214190180026482 al que le corresponde el número 699666141. También incluye información sobre los códecs permitidos para cursar la llamada.

Una vez que Asterisk conoce el IMSI de destino de la llamada, se lo indica a la BTS que va a realizar una llamada con dicho IMSI, con el mensaje *Trying* final:

```
▽ Session Initiation Protocol (100)
  ▽ Status-Line: SIP/2.0 100 Trying
      Status-Code: 100
      [Resent Packet: False]
      [Request Frame: 699]
      [Response Time (ms): 0]
  ▽ Message Header
    ▷ To:  <sip:IMSI214190180026482@127.0.0.1:5062>;tag=OBTSarhagtrxbeqrpcia
    ▷ From: "699666140" <sip:699666140@127.0.0.1>;tag=as53da5cdb
    ▷ Via: SIP/2.0/UDP 127.0.0.1:5060;branch=z9hG4bK669a7221
      Call-ID: 5a360f7b6321ca32487c9df415be5e14@127.0.0.1:5060
    ▷ CSeq: 102 INVITE
    ▷ Contact: <sip:IMSI214190180026482@127.0.0.1:5062>;expires=3600
      User-Agent: OpenBTS 5.0-master Build Date 2015-01-12T18:50:06
      Content-Length: 0
```

**113. MENSAJE DE ASTERISK A LA BTS PARA QUE REALICE BUSQUE AL MS AL QUE VA DESTINADA LA LLAMADA**

Se puede observar cómo en el campo "*To*:", Asterisk le indica a la BTS que el llamado es el abonado cuyo IMSI es 214190180026482.

Tras esto, la BTS envía un mensaje por el TS0 para indicar a todos los MS en su zona de cobertura que va a realizarse una llamada:

```
LAPDm          87 I, N(R)=3, N(S)=1(DTAP) (CC) Call Proceeding
```

**114. MENSAJES PARA INDICAR EL INICIO DE LLAMADA BTS-MS Y MS-BTS**

El mensaje en detalle se ve que es enviado por el TS0 y que es un aviso a los móviles sobre que va a llegarles una llamada:

```
▷ GSM TAP Header, ARFCN: 2 (Downlink), TS: 0, Channel: SDCCH/4 (0)
▷ Link Access Procedure, Channel Dm (LAPDm)
▽ GSM A-I/F DTAP - Call Proceeding
  ▷ Protocol Discriminator: Call Control; call related SS messages
    00.. .... = Sequence number: 0
    ..00 0010 = DTAP Call Control Message Type: Call Proceeding (0x02)
```

**115. MENSAJE DE LA BTS A LOS MS PARA INDICAR LA LLEGADA DE UNA LLAMADA.**

Una vez se ha indicado la llegada de una llamada, la BTS le asigna al MS llamante el TS3 por el que se comunicará con la BTS como se puede ver a continuación:

```
LAPDm          87 I, N(R)=3, N(S)=2(DTAP) (RR) Assignment Command
```

**116. MENSAJE DE ASIGNACIÓN DEL CANAL FÍSICO PARA CURSAR LA LLAMADA. BTS-MS**

```
▽ GSM A-I/F DTAP - Assignment Command
  ▷ Protocol Discriminator: Radio Resources Management messages
    DTAP Radio Resources Management Message Type: Assignment Command (0x2e)
  ▽ Channel Description 2 - Description of the First Channel, after time
      0000 1... = TCH/F + FACCH/F and SACCH/F
      .... .011 = Timeslot: 3
      010. .... = Training Sequence: 2
      ...0 .... = Hopping channel: No
      .... 00.. = Spare
      Single channel : ARFCN 2
  ▽ Power Command
      0... .... = Spare: 0
      .0.. .... = EPC_mode: Channel(s) not in EPC mode
      ..0. .... = FPC_EPC: FPC not in use/C not in use for uplink power control
      ...0 0000 = POWER LEVEL: 0
  ▽ Channel Mode - Mode of the First Channel(Channel Set 1)
      Element ID: 0x63
      Channel Mode: speech full rate or half rate version 1(GSM FR or GSM HR) (1)
```

**117. DETALLE MENSAJE DE ASIGNACIÓN DE TS PARA CURSAR LA LLAMADA**

En el detalle se observa que la BTS le indica el TS3, la secuencia de entrenamiento para ecualizar el canal radio es la número 2 conocida por MS y BTS. A este mensaje le responde el teléfono llamante con el siguiente mensaje:

```
LAPDm          81 I, N(R)=0, N(S)=0(DTAP) (RR) Assignment Complete
```

**118. CONFIRMACIÓN DE LA ASIGNACIÓN DEL CANAL**

```
▽ GSM A-I/F DTAP - Assignment Complete
  ▷ Protocol Discriminator: Radio Resources Management messages
    DTAP Radio Resources Management Message Type: Assignment Complete (0x29)
  ▽ RR Cause
      RR cause value: Normal event (0)
```

**119. CONFIRMACIÓN DEL MS DE LA ASIGNACIÓN DE TS PARA LA LLAMADA**

Con el mensaje anterior el móvil llamante dispone de una canal radio dedicado para la llamada, después el móvil llamado responde al mensaje de llamada:

```
LAPDm          81 U P, func=SABM(DTAP) (RR) Paging Response
```

**120. MENSAJES DE RESPUESTA A LA INDICACIÓN DE LLAMADA**

```
▽ GSM A-I/F DTAP - Paging Response
  ▷ Protocol Discriminator: Radio Resources Management messages
    DTAP Radio Resources Management Message Type: Paging Response (0x27)
    0000 .... :  Spare
  ▽ Ciphering Key Sequence Number
      .... 0... :  Spare
      .... .000 :  Ciphering Key Sequence Number: 0
  ▷ Mobile Station Classmark 2
  ▷ Mobile Identity - IMSI (214190180026482)
```

Se puede observar como en la respuesta, el móvil llamado, envía su IMSI y los datos para el cifrado de la comunicación. A ese mensaje de respuesta del móvil, la BTS envía un mensaje en el que indica el número que origina la llamada como se puede ver en el mensaje siguiente:

```
LAPDm          87 I, N(R)=0, N(S)=0(DTAP) (CC) Setup
```

**121. MENSAJE CON NÚMERO LLAMANTE**

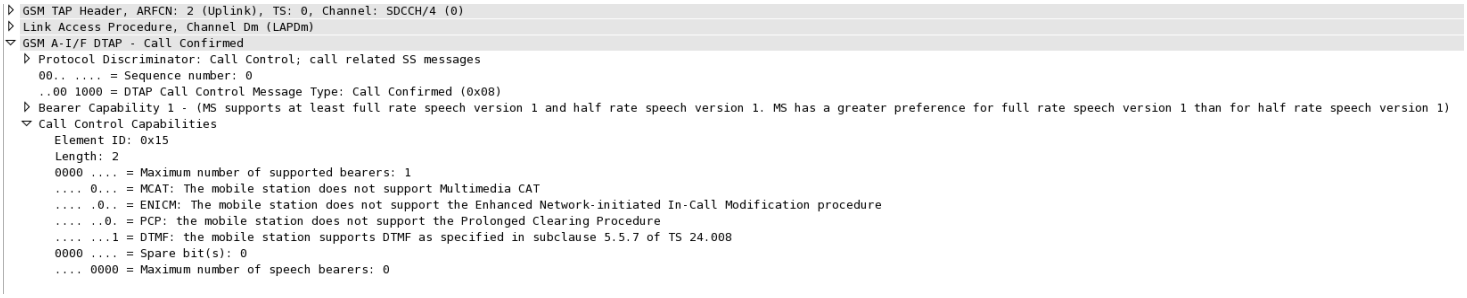
```
▷ GSM TAP Header, ARFCN: 2 (Downlink), TS: 0, Channel: SDCCH/4 (0)
▷ Link Access Procedure, Channel Dm (LAPDm)
▽ GSM A-I/F DTAP - Setup
  ▷ Protocol Discriminator: Call Control; call related SS messages
    00.. .... = Sequence number: 0
    ..00 0101 = DTAP Call Control Message Type: Setup (0x05)
  ▷ Calling Party BCD Number - (699666140)
```

**122. DETALLE DEL MENSAJE CON NÚMERO LLAMANTE**

En este detalle del mensaje se puede observar el número de teléfono que origina la llamada 699666140 y cómo la BTS lo publica en el TS0 porque aún no tiene asignado el móvil destino un canal físico. Cuando el móvil destino obtiene ese mensaje, le responde a la BTS para confirmar que está disponible para recibirla:

```
LAPDm          81 I, N(R)=1, N(S)=1(DTAP) (CC) Call Confirmed
```

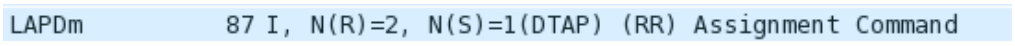
**123. MENSAJE DE CONFIRMACIÓN DE RECEPCIÓN DE LLAMADA**



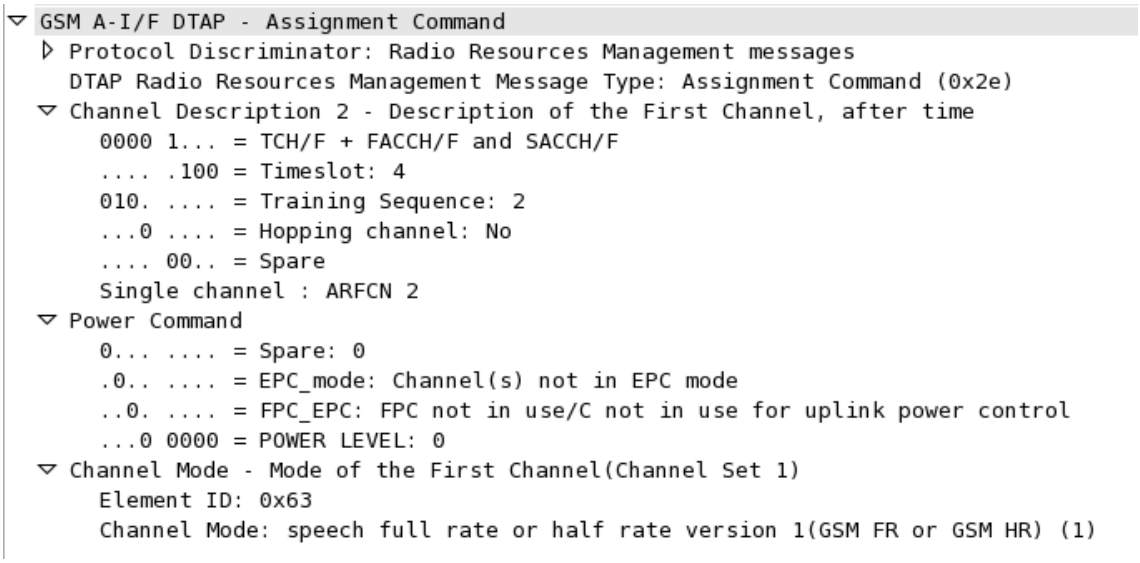

**124. DETALLE DEL MENSAJE DE CONFIRMACIÓN DE RECEPCIÓN DE LLAMADA**

En el mensaje anterior, el móvil le indica sus características a la BTS, como por ejemplo el códec y que prefiere realizar la llamada usando un canal de velocidad completa.

Una vez que BTS y móvil tienen conocimiento de que puede recibir la llamada, la BTS le asigna un canal físico para la misma y el MS le confirma el uso de ese TS como se puede ver en los siguientes mensajes:

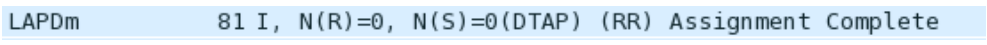



**125. MENSAJES DE ASIGNACIÓNDE CANAL PARA RECEPCIÓN DE LLAMADA**

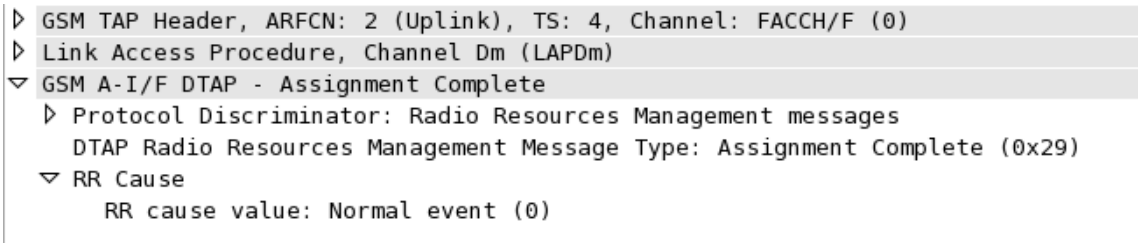



**126. DETALLE DE LA ASIGNACIÓN DE TS POR PARTE DE LA BTS**

En este mensaje la BTS le asigna el TS4 al móvil llamado y que utilice la secuencia de entrenamiento para la ecualización del canal número dos. A este mensaje le responde el MS con el siguiente mensaje:

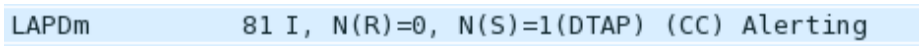



**127. CONFIRMACIÓN DE LA ASIGNACIÓN DE CANAL**

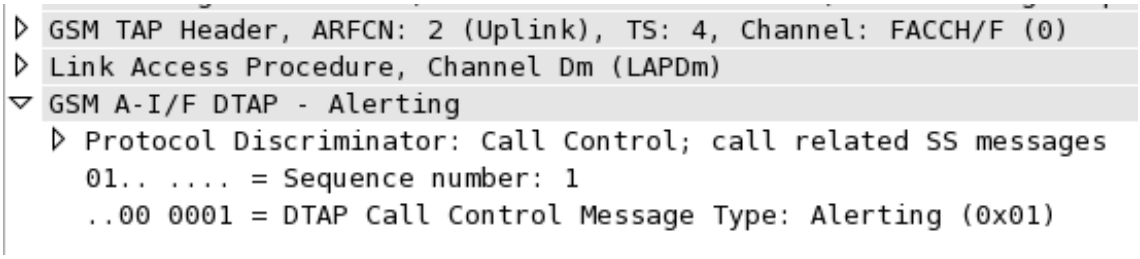



**128. DETALLE DEL MENSAJE DE CONFIRMACIÓN**

Una vez tiene el canal asignado, la BTS envía un mensaje de alerta al teléfono llamado para que éste comience a sonar y/o vibrar para que el abonado pueda descolgar el mismo y comenzar la conversación entre ambos móviles.

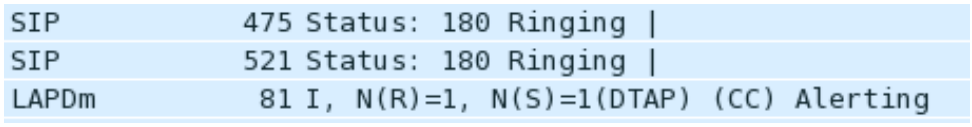



**129. MENSAJE DE ALERTA DE LA BTS AL MS LLAMADO**




**130.DETALLE DEL MENSAJE DE ALERTA**

También la BTS indica a Asterisk que tanto llamante como llamado está en proceso de iniciar la conversación por medio de los mensajes SIP "*Ringing*". El último mensaje de alerta es el correspondiente al móvil llamante, para que comience a sonar el tono de llamada en proceso.




**131. MENSAJES SIP DE LLAMADA EN PROCESO**

Vamos a mostrar el detalle de los mensajes anteriores para que se verifique que cada uno corresponde a una comunicación. Uno entre llamante y Asterisk y el otro entre Asterisk y llamado.

```
▽ Session Initiation Protocol (180)
  ▽ Status-Line: SIP/2.0 180 Ringing
      Status-Code: 180
      [Resent Packet: False]
      [Request Frame: 699]
      [Response Time (ms): 7752]
  ▽ Message Header
    ▷ To:  <sip:IMSI214190180026482@127.0.0.1:5062>;tag=OBTSarhagtrxbeqrpcia
    ▷ From: "699666140" <sip:699666140@127.0.0.1>;tag=as53da5cdb
    ▷ Via: SIP/2.0/UDP 127.0.0.1:5060;branch=z9hG4bK669a7221
      Call-ID: 5a360f7b6321ca32487c9df415be5e14@127.0.0.1:5060
    ▷ CSeq: 102 INVITE
    ▷ Contact: <sip:IMSI214190180026482@127.0.0.1:5062>;expires=3600
      User-Agent: OpenBTS 5.0-master Build Date 2015-01-12T18:50:06
      Content-Length: 0
```

**132. MENSAJE DE ASTERISK A LA BTS CON DESTINO EL MÓVIL LLAMADO**

```
▽ Session Initiation Protocol (180)
  ▽ Status-Line: SIP/2.0 180 Ringing
      Status-Code: 180
      [Resent Packet: False]
      [Request Frame: 683]
      [Response Time (ms): 7776]
  ▽ Message Header
    ▷ Via: SIP/2.0/UDP 127.0.0.1:5062;branch=z9hG4bKOBTSvmfxoszvwofkihga;received=127.0.0.1
    ▷ From: <sip:IMSI460011901250000@127.0.0.1:5062>;tag=OBTSrjyziylnzdvrcseg
    ▷ To: <sip:699666141@127.0.0.1>;tag=as3dcf1fd9
      Call-ID: 46e661f57abab95d
    ▷ CSeq: 486247 INVITE
      Server: Asterisk PBX 11.7.0.4
      Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO, PUBLISH
      Supported: replaces, timer
    ▷ Contact: <sip:699666141@127.0.0.1:5060>
      Content-Length: 0
```

**133. MENSAJE ENTRE BTS DE PARTE DEL MÓVIL LLAMANTE HACIA ASTERISK**

```
▽ GSM A-I/F DTAP - Alerting
  ▷ Protocol Discriminator: Call Control; call related SS messages
    00.. .... = Sequence number: 0
    ..00 0001 = DTAP Call Control Message Type: Alerting (0x01)
  ▽ Progress Indicator
      Element ID: 0x1e
      Length: 2
      1... .... = Extension: No Extension
      .11. .... = Coding standard: standard defined for the GSM PLMNS as described below (0x03)
      ...0 .... = Spare bit(s): 0
      .... 0000 = Location: User (0x00)
      1... .... = Extension: No Extension
      .100 0000 = Progress description: Queueing (64)
```

**134. MENSJA DE ALERTA DE LA BTS AL MÓVIL LLAMANTE**

Con este grupo de 4 mensajes entre MS1-BTS, BTS-Asterisk, Asterisk-BTS, BTS-MS2 ambos abonados están en proceso de poder comunicarse. El siguiente paso es establecer el canal de voz cuando el llamado descuelgue el teléfono. Los mensajes siguientes son los relativos a la confirmación de cursar la llamada.

```
LAPDm          81 I, N(R)=0, N(S)=2(DTAP) (CC) Connect
SIP/SDP       817 Status: 200 OK |
SIP           469 Request: ACK sip:IMSI214190180026482@127.0.0.1:5062 |
SIP/SDP       721 Status: 200 OK |
SIP           419 Request: ACK sip:699666141@127.0.0.1:5060 |
LAPDm          81 I, N(R)=1, N(S)=2(DTAP) (CC) Connect
LAPDm          81 I, N(R)=3, N(S)=0(DTAP) (CC) Connect Acknowledge
LAPDm          81 I, N(R)=3, N(S)=1(DTAP) (CC) Connect Acknowledge
```

**135. MENSJAES QUE CONFIRMAN CURSAR LA LLAMADA**

Los mensajes que confirman que se va a cursar la llamada comienzan por el mensaje de conexión del móvil llamado, que se envía cuando el abonado descuelga el mismo. Cuando la BTS recibe ese mensaje, le responde a Asterisk con el mensaje de OK al mensaje de "Ringing" anterior y la centralita envía un ACK a la BTS para que pueda dar comienzo la transmisión de voz

```
▷ GSM TAP Header, ARFCN: 2 (Uplink), TS: 4, Channel: FACCH/F (0)
▷ Link Access Procedure, Channel Dm (LAPDm)
▽ GSM A-I/F DTAP - Connect
  ▷ Protocol Discriminator: Call Control; call related SS messages
    00.. .... = Sequence number: 0
    ..00 0111 = DTAP Call Control Message Type: Connect (0x07)
```

**136. MENSAJE DE CONFIRMACIÓN DE DESCOLGADO DEL TELÉFONO**

En este mensaje se observa cómo lo emite el móvil llamado TS4 y uplink.

```
▽ Session Initiation Protocol (200)
  ▽ Status-Line: SIP/2.0 200 OK
      Status-Code: 200
      [Resent Packet: False]
      [Request Frame: 699]
      [Response Time (ms): 12811]
  ▽ Message Header
    ▷ To:  <sip:IMSI214190180026482@127.0.0.1:5062>;tag=OBTSarhagtrxbeqrpcia
    ▷ From: "699666140" <sip:699666140@127.0.0.1>;tag=as53da5cdb
    ▷ Via: SIP/2.0/UDP 127.0.0.1:5060;branch=z9hG4bK669a7221
      Call-ID: 5a360f7b6321ca32487c9df415be5e14@127.0.0.1:5060
    ▷ CSeq: 102 INVITE
    ▷ Contact: <sip:IMSI214190180026482@127.0.0.1:5062>;expires=3600
    ▷ P-PHY-Info: OpenBTS; IMSI=214190180026482 TA=0 TE=0.096858 UpRSSI=-49.762867 TxPwr=5 DnRSSIdBm=-48 time=1423132402.327
      P-Access-Network-Info: 3GPP-GERAN; cgi-3gpp=0010103e8000a
      User-Agent: OpenBTS 5.0-master Build Date 2015-01-12T18:50:06
      Content-Type: application/sdp
      Content-Length: 135
  ▷ Message Body
```

**137. MENSAJE SIP DE OK AL INVITE**

Este mensaje lo origina Asterisk, de parte del móvil llamante, hacia la BTS para el móvil llamado. Indicando que se ha recibido el mensaje "INVITE" enviado al comienzo del proceso de la llamada por parte del móvil llamante.

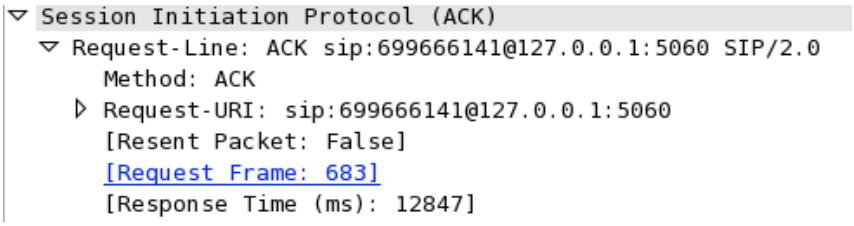
```
▽ Session Initiation Protocol (ACK)
  ▽ Request-Line: ACK sip:IMSI214190180026482@127.0.0.1:5062 SIP/2.0
      Method: ACK
    ▷ Request-URI: sip:IMSI214190180026482@127.0.0.1:5062
      [Resent Packet: False]
      [Request Frame: 699]
      [Response Time (ms): 12812]
```

**138. CONFIRMACIÓN DEL RINGING**

Este mensaje lo envía la BTS a la centralita para confirmar la recepción del "RINGING" entre la centralita y el móvil llamado.

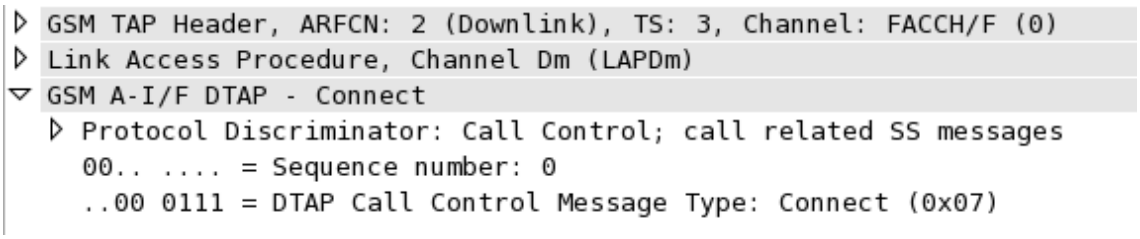
**139. MENSAJE DE OK AL INVITE DE LLAMANTE**

Este mensaje es similar a la confirmación del INVITE previa, como en el caso anterior pero esta vez es enviado por la BTS, de parte del móvil llamante, a la centralita, de parte del móvil llamado.



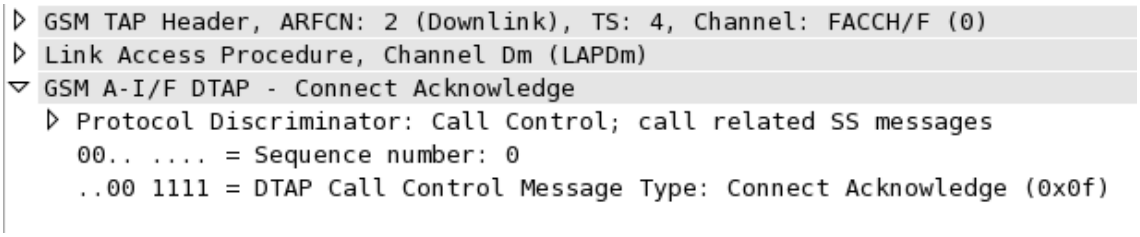

**140. MENSAJE DE CONFIRMACIÓN DEL MENSAJE RINGING**

Mensaje de confirmación de RINGING enviado por la centralita, de parte del móvil llamante, hacia la BTS con destino al móvil llamado.




**141. CONFIRMACIÓN DE LA COMUNICACIÓN DE LA BTS AL LLAMANTE**

Mensaje enviado por la BTS al móvil llamante para indicar que va a dar comienzo la comunicación.




**142. CONFIRMACIÓN DE LA LLAMADA DE LA BTS AL MS LLAMADO**

Mensaje enviado por la BTS al móvil llamado para indicarle que va a dar comienzo la transmisión de voz.

```
▷ GSM TAP Header, ARFCN: 2 (Uplink), TS: 3, Channel: FACCH/F (0)
▷ Link Access Procedure, Channel Dm (LAPDm)
▽ GSM A-I/F DTAP - Connect Acknowledge
  ▷ Protocol Discriminator: Call Control; call related SS messages
    00.. .... = Sequence number: 0
    ..00 1111 = DTAP Call Control Message Type: Connect Acknowledge (0x0f)
```

**143. CONFIRMACIÓN DE LA LLAMADA DEL LLAMANTE A LA BTS**

Confirmación por parte del móvil llamante a la BTS de que está listo para cursar la llamada.

Una vez los dos interlocutores han realizado la llamada, uno de ellos cuelga el teléfono. En nuestro caso el primero en colgar es el mismo que origina la llamada. Los mensajes para liberalizar los recursos de la red son los siguientes:

```
LAPDm          81 I, N(R)=3, N(S)=2(DTAP) (CC) Disconnect
SIP           472 Request: BYE sip:699666141@127.0.0.1:5060 |
SIP           472 Status: 200 OK |
SIP           525 Request: BYE sip:IMSI214190180026482@127.0.0.1:5062 |
SIP           403 Status: 200 OK |
LAPDm          81 I, N(R)=3, N(S)=3(DTAP) (CC) Release
LAPDm          81 I, N(R)=3, N(S)=1(DTAP) (CC) Disconnect
LAPDm          81 I, N(R)=4, N(S)=3(DTAP) (CC) Release Complete
LAPDm          81 I, N(R)=2, N(S)=3(DTAP) (CC) Release
```

**144. INTERCAMBIO DE MENSAJES AL FINALIZAR UNA LLAMADA**

A continuación se mostrará en detalle los mensajes intercambiados que se han mostrado.

```
▷ GSM TAP Header, ARFCN: 2 (Uplink), TS: 3, Channel: FACCH/F (0)
▷ Link Access Procedure, Channel Dm (LAPDm)
▽ GSM A-I/F DTAP - Disconnect
  ▷ Protocol Discriminator: Call Control; call related SS messages
    01.. .... = Sequence number: 1
    ..10 0101 = DTAP Call Control Message Type: Disconnect (0x25)
  ▽ Cause - (16) Normal call clearing
      Length: 2
      1... .... = Extension: No Extension
      .11. .... = Coding standard: Standard defined for the GSM PLMNS
      ...0 .... = Spare bit(s): 0
      .... 0000 = Location: User
      1... .... = Extension: No Extension
      .001 0000 = Cause: (16) Normal call clearing
```

**145. LLAMANTE CUELGA EL MÓVIL**

Primer mensaje que envía el móvil que decide finalizar la llamada. Como dato interesante en el mensaje es la causa de la finalización, que en nuestro caso es una finalización normal, porque es el usuario el que ha decidido terminar dicha llamada.

```
▽ Session Initiation Protocol (BYE)
  ▽ Request-Line: BYE sip:699666141@127.0.0.1:5060 SIP/2.0
      Method: BYE
    ▷ Request-URI: sip:699666141@127.0.0.1:5060
      [Resent Packet: False]
  ▽ Message Header
    ▷ To: <sip:699666141@127.0.0.1>;tag=as3dcf1fd9
    ▷ From:  <sip:IMSI460011901250000@127.0.0.1:5062>;tag=OBTSrjyziylnzdvrcseg
    ▷ Via: SIP/2.0/UDP 127.0.0.1:5062;branch=z9hG4bKOBTSwjsebnkuygiqcfad
      Call-ID: 46e661f57abab95d
    ▷ CSeq: 486248 BYE
      Max-Forwards: 70
      User-Agent: OpenBTS 5.0-master Build Date 2015-01-12T18:50:06
    ▷ Reason: Q.850;cause=16 ;text="Normal_Call_Clearing"
      Content-Length: 0
```

**146. MENSAJE DE CIERRE DE LA CONEXIÓN ENTRE BTS Y ASTERISK**

Cuando la BTS recibe el mensaje del móvil de finalizar la llamada, ésta envía el mensaje BYE a la centralita para terminar la comunicación.

```
▽ Session Initiation Protocol (200)
  ▽ Status-Line: SIP/2.0 200 OK
      Status-Code: 200
      [Resent Packet: False]
      [Request Frame: 23853]
      [Response Time (ms): 0]
      [Release Time (ms): 0]
```

**147. CONFIRMACIÓN POR PARTE DE ASTERISK AL CIERRE DE LA CONEXÍON.**

La centralita confirma la recepción del mensaje BYE por medio del mensaje OK anterior.

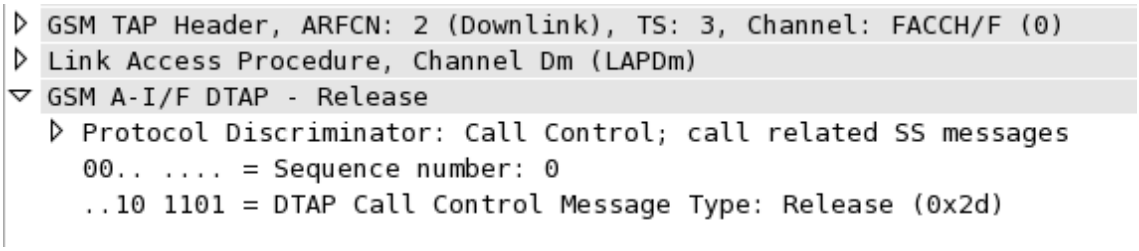
```
▽ Session Initiation Protocol (BYE)
  ▽ Request-Line: BYE sip:IMSI214190180026482@127.0.0.1:5062 SIP/2.0
      Method: BYE
    ▷ Request-URI: sip:IMSI214190180026482@127.0.0.1:5062
      [Resent Packet: False]
  ▽ Message Header
    ▷ Via: SIP/2.0/UDP 127.0.0.1:5060;branch=z9hG4bK57f74f6f
      Max-Forwards: 70
    ▷ From: "699666140" <sip:699666140@127.0.0.1>;tag=as53da5cdb
    ▷ To: <sip:IMSI214190180026482@127.0.0.1:5062>;tag=OBTSarhagtrxbeqrpcia
      Call-ID: 5a360f7b6321ca32487c9df415be5e14@127.0.0.1:5060
    ▷ CSeq: 103 BYE
      User-Agent: Asterisk PBX 11.7.0.4
    ▷ Reason: Q.850;cause=16
    ▷ X-Asterisk-HangupCause: Normal Clearing
    ▷ X-Asterisk-HangupCauseCode: 16
      Content-Length: 0
```

**148. INDICACIÓN DE ASTERISK A LA BTS DEL CIERRE DE LA CONVERSACIÓN POR PARTE DEL LLAMANTE.**

Ahora la centralita indica a la BTS que la comunicación ha terminado por medio de otro mensaje BYE, puesto que hay dos canales de comunicaciones, uno entre llamante y centralita y otro entre centralita y llamado.

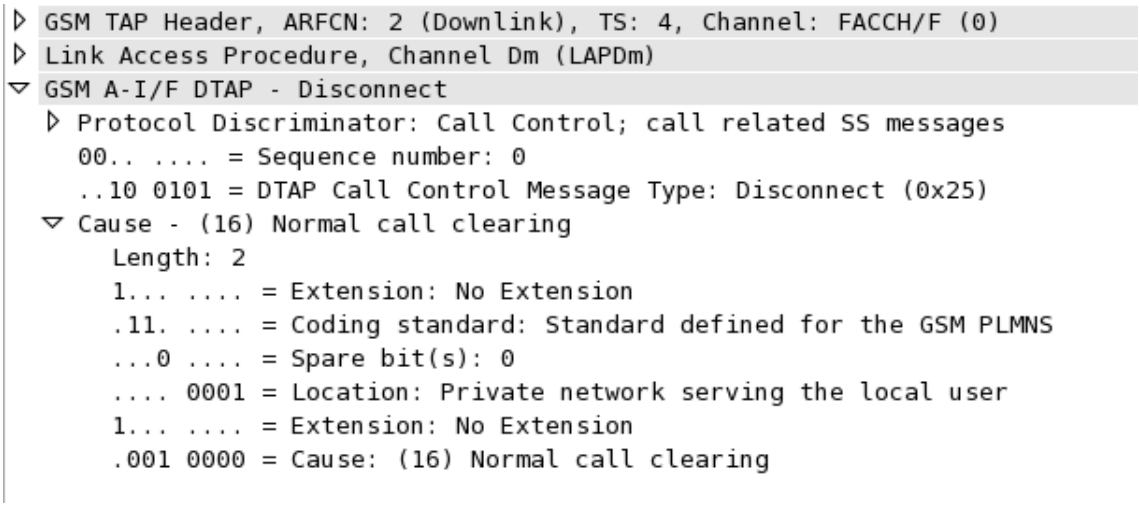
**149. CONFIRMACIÓN DE LA BTS A ASTERISK DE LA RECEPCIÓN DEL MENSAJE DE CIERRE DE LA COMUNICACIÓN**

La BTS confirma la recepción del mensaje de finalización de la llamada y procederá con el proceso de liberación de los TS en uso.



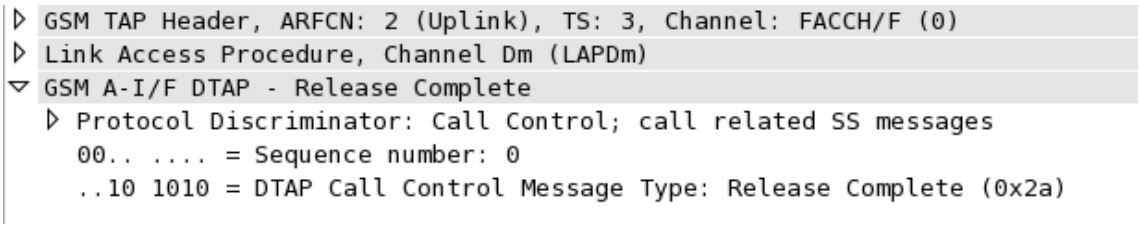

**150. MENSAJE DE LA BTS AL MÓVIL LLAMANTE DE QUE HA TERMINADO LA COMUNICACIÓN.**

Comienza enviando un mensaje al móvil que ha colgado la llamada para que comience la liberación de los recursos utilizados.



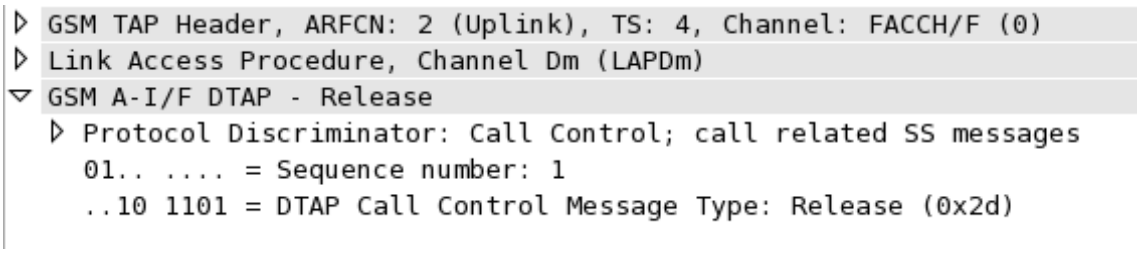

**151. MENSAJE DE LA BTS AL LLAMADO PARA LA DESCONEXIÓN DE LA RED**

La BTS indica al móvil llamado que se ha terminado la llamada de forma normal, para que éste pueda reproducir el sonido equivalente a la finalización normal de una llamada.



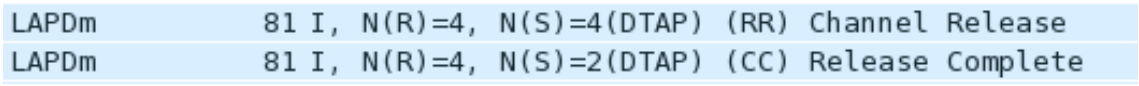

**152. CONFIRMACIÓN DEL MÓVIL LLAMANTE DE LA FINALIZACIÓN DE LA LLAMADA.**

El móvil que ha realizado la llamada, le confirma a la BTS la liberación de los recursos por medio del mensaje anterior.

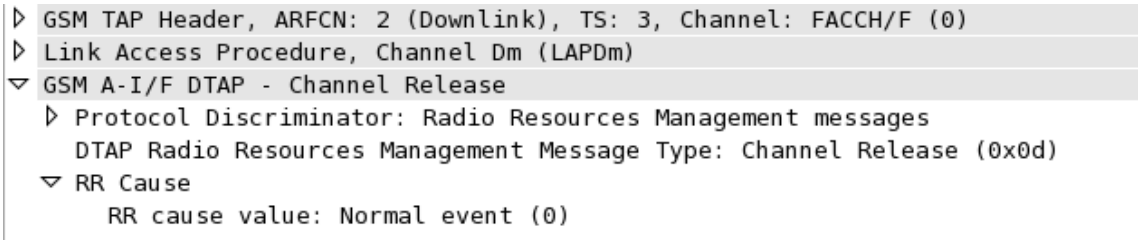



153. MENSAJE DEL MÓVIL LLAMADO A LA BTS PARA INDICAR EL FIN DE LA COMUNICACIÓN

Una vez que el abonado llamado cuelga también su móvil o pasado cierto tiempo, se finaliza la llamada en él y el móvil envía un mensaje a la BTS para que pueda liberar los recursos también. El proceso de liberación de recursos continúa con los siguientes mensajes:

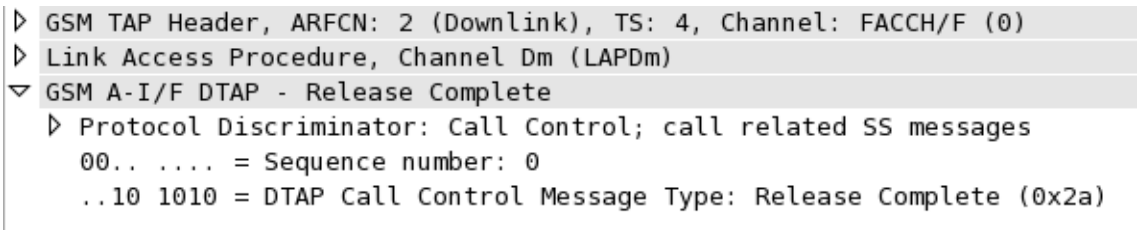



154. MENSAJES PARA DEJAR LIBRE EL CANAL RADIO



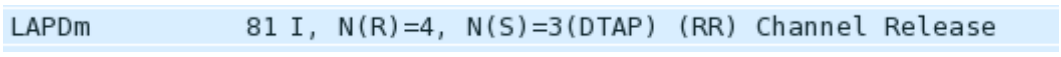

155. INDICACION DE LA BTS AL LLAMANTE DE QUE SE VA A LIBERAR EL CANAL RADIO

Este primero le indica al móvil llamante que libere el canal radio.




156. CONFIRMACIÓN DE LA BTS AL MÓVIL LLAMAO DE LA LIBERALICACIÓN DEL CIRCUITO DE LA LLAMADA

En este caso la BTS le confirma al móvil llamante que ha procedido a la liberación de los diferentes recursos utilizados durante la llamada.




157. MENSAJE DE LIBERACIÓN DEL CANAL RADIO POR PARTE DEL MOVIL LLAMADO

```
▷ GSM TAP Header, ARFCN: 2 (Downlink), TS: 4, Channel: FACCH/F (0)
▷ Link Access Procedure, Channel Dm (LAPDm)
▽ GSM A-I/F DTAP - Channel Release
  ▷ Protocol Discriminator: Radio Resources Management messages
    DTAP Radio Resources Management Message Type: Channel Release (0x0d)
  ▽ RR Cause
      RR cause value: Normal event (0)
```

**158. DETALLE DEL MENSAJE DE LA LIBERACIÓN DEL CANAL RADIO.**

Finalmente el móvil llamado libera los recursos radio que tenía asignados.

### 4.3.4 ANÁLISIS DE LA CALIDAD DE LA LLAMADA

Una vez vistos los mensajes intercambiados entre los diferentes elementos de la red GSM creada con OpenBTS, gracias a la herramienta de análisis de mensajes Wireshak utilizada, podremos ver también parámetros relativos a la transmisión del audio por parte del móvil. Como se puede ver a continuación:

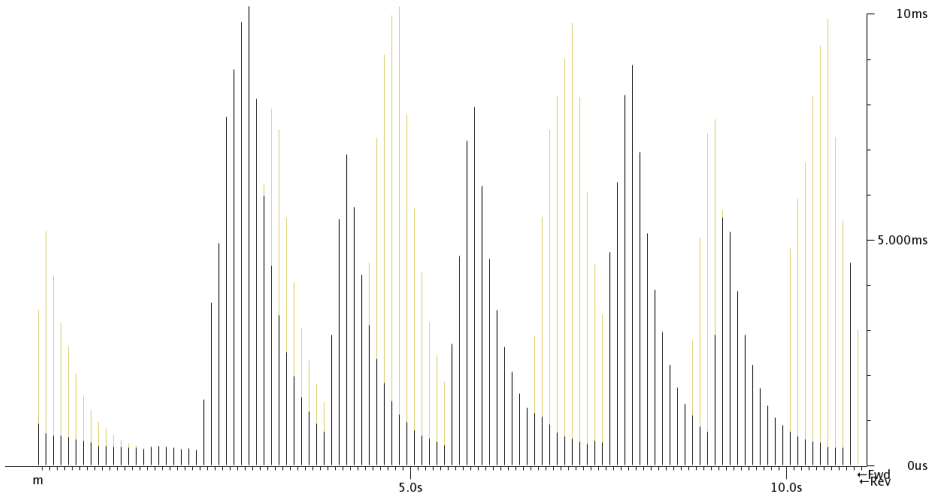
```
Max delta = 40.63 ms at packet no. 13733
Max jitter = 10.37 ms. Mean jitter = 2.22 ms.
Max skew = 22.52 ms.
```

**159. ESTADÍSTICAS DE LAS MEDIDAS DE LOS PARÁMETROS DE LA CONVERSACIÓN.**

El software nos ofrece las estadísticas siguientes: retardo máximo de la conversación de 40.63 ms; el máximo *jitter* es de 10.37ms y con un valor medio de 2.2ms; y un máximo de *skew* de 22.52ms.

Todos estos factores afectarán a la calidad de la llamada objetiva de la llamada, así como a la calidad percibida por el abonado, ya que un retardo muy alto impide una comunicación fluida por parte de ambos interlocutores.

La aplicación también nos permite mostrar los datos anteriores en una gráfica como la siguiente, en la que se muestra la evolución del *jitter* en ambos sentidos:



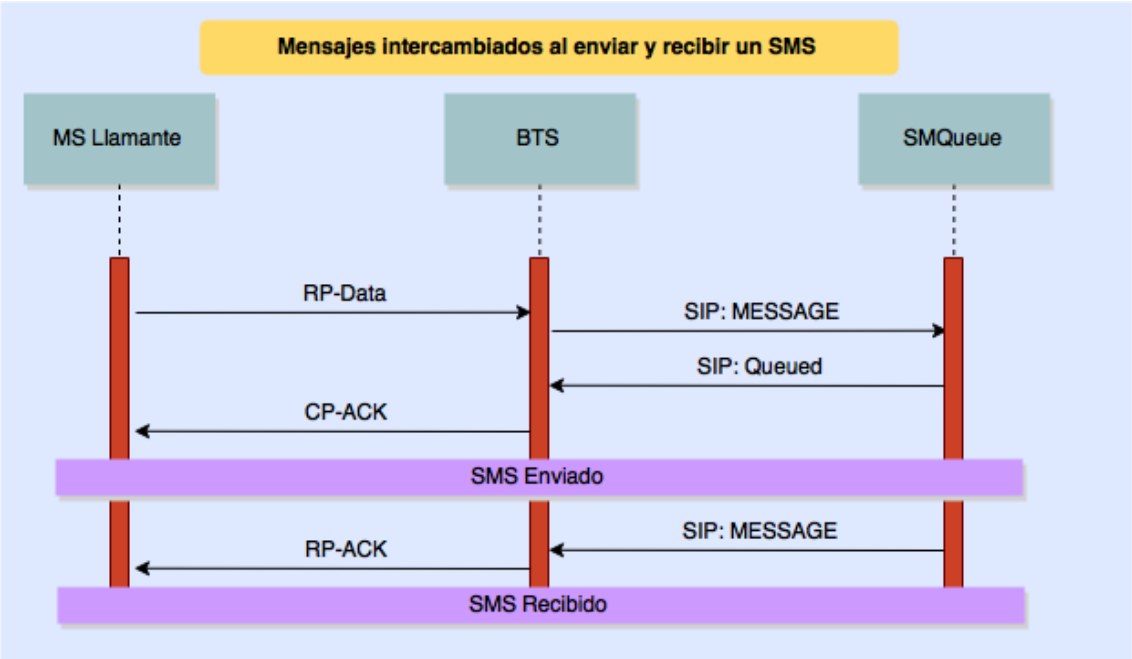

**160. EVOLUCIÓN DEL JITTER EN LA LLAMADA**

Se observa cierta periodicidad, debida seguramente a los diferentes búferes del móvil origen, BTS, Asterisk, y móvil destino.

Una vez analizadas las llamadas, se analizará el envío y recepción de SMS.

### 4.3.5 ENVÍO DE SMS

En el apartado anterior se ha estudiado con detalle el intercambio de mensajes necesario para poder cursar una llamada con el sistema OpenBTS. Otra de las mayores utilidades de la red GSM es el envío y recepción de mensajes cortos o SMS y a continuación se mostrará en detalle el intercambio de mensajes entre los diferentes elementos de la red. Comenzaremos con el envío de un SMS a un número de test, el 411, y éste mismo número nos responderá al móvil con el mismo mensaje que hemos enviado.




**161. MENSAJES INTERCAMBIADOS AL ENVIAR Y RECIBIR UN SMS**

Comenzamos con el intercambio de mensajes correspondiente al envío de un SMS:

```
GSM SMS        81 I, N(R)=0, N(S)=2(DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to Network)
SIP           647 Request: MESSAGE sip:smsc@127.0.0.1:5063 | (RP)
SIP           302 Status: 202 Queued |
```

**162. MENSAJES RESPONSABLES DEL ENVÍO DE UN SMS**

Los mensajes son: el que envía el móvil a la BTS; el que envía la BTS al servidor de SMS; y la respuesta de éste a la BTS. Más en detalle los mensajes anteriores:

```
▷ GSM TAP Header, ARFCN: 2 (Uplink), TS: 0, Channel: SDCCH/4 (0)
▷ Link Access Procedure, Channel Dm (LAPDm)
▷ GSM A-I/F DTAP - CP-DATA
▷ GSM A-I/F RP - RP-DATA (MS to Network)
▽ 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: 13
  ▷ TP-Destination-Address - (9010)
  ▷ TP-PID: 40
  ▷ TP-DCS: 0
    TP-User-Data-Length: (1) depends on Data-Coding-Scheme
  ▷ TP-User-Data
```

**163. MENSJAE ENTRE MS Y BTS CON EL ENVÍO DE UN SMS**

Este es un mensaje enviado por el móvil a la BTS a través de TS0, por lo que para enviar SMS no es necesario el proceso de solicitar un canal de tráfico.

```
▽ Session Initiation Protocol (MESSAGE)
  ▽ Request-Line: MESSAGE sip:smsc@127.0.0.1:5063 SIP/2.0
      Method: MESSAGE
    ▷ Request-URI: sip:smsc@127.0.0.1:5063
      [Resent Packet: False]
  ▽ Message Header
    ▷ To:  <sip:smsc@127.0.0.1>
    ▷ From:  <sip:IMSI460011901250000@127.0.0.1:5062>;tag=OBTSkcfnrjayvlqwwega
    ▷ Via: SIP/2.0/UDP 127.0.0.1:5062;branch=z9hG4bKOBTSgnkstgflprxhkutc
      Call-ID: 464dd50f17a0cd75
    ▷ CSeq: 486244 MESSAGE
    ▷ Contact: <sip:IMSI460011901250000@127.0.0.1:5062>;expires=3600
      Max-Forwards: 70
    ▷ P-Preferred-Identity: <sip:IMSI460011901250000@127.0.0.1>
      User-Agent: OpenBTS 5.0-master Build Date 2015-01-12T18:50:06
      Content-Type: application/vnd.3gpp.sms
      Content-Length: 80
  ▷ Message Body
```

**164. MENSAJE SIP ENTRE LA BTS Y SMQUEUE**

Una vez que el SMS ha llegado a la BTS, ésta lo envía al servidor de SMS, que en nuestro caso, con OpenBTS es SMQUEUE indicándole quien envía el mensaje y el tipo de mensaje es un SMS de la red móvil GSM, "3gpp.sms".

```
▽ Session Initiation Protocol (202)
  ▽ Status-Line: SIP/2.0 202 Queued
      Status-Code: 202
      [Resent Packet: False]
      [Request Frame: 1020]
      [Response Time (ms): 15]
```

**165. MENSAJE SIP ENTRE SMQUEUE Y EL DESTINO**

El servidor de mensajes le responde a la BTS indicándole que ya ha colocado en cola el SMS a la espera de enviarlo a su receptor.

```
LAPDm          87 I, N(R)=3, N(S)=0(DTAP) (SMS) CP-ACK
```

**166. MENSAJE DE LA BTS AL MS CON LA CONFIRMACIÓN DE LA RECEPCIÓN DEL SMS**

Por último la BTS informa al móvil de que su mensaje ha sido recibido por el servidor de mensajes y será enviado cuando le toque su turno dentro de la cola de mensajes.

```
▷ GSM TAP Header, ARFCN: 2 (Downlink), TS: 0, Channel: SDCCH/4 (0)
▷ Link Access Procedure, Channel Dm (LAPDm)
▽ GSM A-I/F DTAP - CP-ACK
  ▷ Protocol Discriminator: SMS messages
    DTAP Short Message Service Message Type: CP-ACK (0x04)
```

**167. DETALLE DE LA CONFIRMACIÓN DE RECEPCIÓN DEL SMS**

Hasta aquí el envío de un SMS por parte de un móvil a un elemento de la red. Ahora el programa encargado de gestionar el número de teléfono 411 envía un mensaje SMS al móvil como respuesta. Para ello comienza enviando un mensaje SIP a la BTS:

```
SIP          450 Request: MESSAGE sip:IMSI460011901250000@127.0.0.1:5062 |  (text/plain)
```

**168. MENSAJE ENTRE ELEMENTO DE LA RED Y LA BTS**

```
▽ Session Initiation Protocol (MESSAGE)
  ▽ Request-Line: MESSAGE sip:IMSI460011901250000@127.0.0.1:5062 SIP/2.0
      Method: MESSAGE
    ▷ Request-URI: sip:IMSI460011901250000@127.0.0.1:5062
      [Resent Packet: False]
  ▽ Message Header
    ▷ Via: SIP/2.0/UDP 127.0.0.1:5063;branch=1;received=smqueue@Range.com
    ▷ From: 411 <sip:411@127.0.0.1>;tag=36002
    ▷ To: <sip:IMSI460011901250000@127.0.0.1>
      Call-ID: N18Vs@127.0.0.1
    ▷ CSeq: 36002 MESSAGE
      Content-Type: text/plain
      Content-Length:   103
  ▽ Message Body
    ▽ Line-based text data: text/plain
        1 queued, cell 0.1, IMSI460011901250000, phonenum 699666140, at Feb  5 11:30:38, 'Hola esto es un test'
```

**169. DETALLE DEL MENSAJE SMS ENVÍADO POR SIP**

Se puede ver que el origen del mensaje es el usuario 411 y el destino es el usuario que envió el SMS al 411. El texto del mensaje no es otro que una copia del mensaje enviado por el móvil al 411, sólo que en este caso va enviado como texto plano y se puede leer con facilidad. Una vez que el mensaje SIP le llega a la BTS, ésta envía el SMS al móvil a través de TS0 como se puede ver en la siguiente captura del mensaje:

```
LAPDm          87 I, N(R)=3, N(S)=1(DTAP) (SMS) CP-DATA (RP) RP-ACK (Network to MS)
```

**170. MENSAJE DE LA BTS AL MÓVIL CON EL SMS**

```
▷ GSM TAP Header, ARFCN: 2 (Downlink), TS: 0, Channel: SDCCH/4 (0)
▷ Link Access Procedure, Channel Dm (LAPDm)
▽ GSM A-I/F DTAP - CP-DATA
  ▽ Protocol Discriminator: SMS messages
      .... 1001 = Protocol discriminator: SMS messages (0x09)
      1... .... = TI flag: allocated by receiver
      .000 .... = TIO: 0
    DTAP Short Message Service Message Type: CP-DATA (0x01)
  ▽ CP-User Data
      Length: 2
      RPDU (not displayed)
▽ GSM A-I/F RP - RP-ACK (Network to MS)
    Message Type RP-ACK (Network to MS)
  ▽ RP-Message Reference
      RP-Message Reference: 0x01 (1)
```

**171. DETALLE DEL MENSAJE ENVIADO POR LA BTS AL MS CON EL SMS**

En el detalle del mensaje se puede comprobar que es un mensaje con origen en la red, es decir enviado por la BTS y con destino el móvil.

Una vez analizados los mensajes intercambiado entre los diferentes elementos de la red GSM, tanto a la hora de realizar llamadas, como a la hora de enviar y recibir SMS, se le dará al proyecto diferentes utilidades comerciales y académicas, aparte de aprender el manejo del analizador vectorial y el análisis del intercambio de mensajes con Wireshark, como se ha visto en este capítulo.

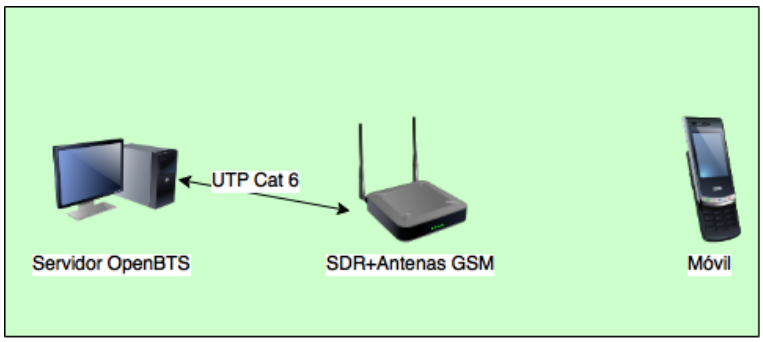
# 5. APLICACIONES

Durante el quinto capítulo del proyecto se mostrará un estudio sobre las posibles utilidades del proyecto realizado, para ello comenzaremos realizando un presupuesto básico de nuestra instalación, y un presupuesto más completo en el que se mostrará el coste de desplegar una red mono BTS. Una vez estudiado el presupuesto pasaremos a comentar las diferentes aplicaciones a las que se le ha encontrado utilidad el proyecto.

## 5.1 PRESUPUESTO DE UNA INSTALACIÓN

Comenzaremos esta parte detallando la partida presupuestaria inicial, es decir, lo mínimo necesario para poder desplegar una estación base con el sistema OpenBTS.

Para poder desplegar el proyecto se necesita muy poco equipamiento hardware, como se ha visto en el capítulo tres.




**172. INSTALACIÓN DE LABORATORIO**

El diagrama anterior muestra la instalación para un laboratorio de pruebas, que tiene el siguiente presupuesto:

| Elemento | Descripción | Unidades | Precio unitario € | Subtotal € |
|---|---|---|---|---|
| SDR | Software Defined Radio. NI 2922 | 1 | 2.680,00 | 2.680,00 |
| Servidor | Servidor PC compatible con, al menos, una interfaz de red Gigabit Ethernet y procesador de, al menos, 2 núcleos. | 1 | 371,07 | 371,07 |
| UTP cat 6 | Digitus Cable de Red RJ45 UTP Cat.6 10/100/1000 Gris 2m | 1 | 2,44 | 2,44 |
| Móvil | Samsung E1270 | 1 | 20,99 | 20,99 |
| SIM | Tarjeta SIM | 1 | 2,82 | 2,82 |
| ANT GSM | Antena GSM con conector SMA | 2 | 9,82 | 19,64 |
| | | | Total (IVA no incluido): | 3.096,96 |

**173. PRESUPUESTO DE UNA INSTALACIÓN DE LABORATORIO**

Una vez visto el presupuesto básico, si queremos dar servicio a una zona más amplia deberemos añadir diferentes elementos a nuestra instalación. Un amplificador GSM y un duplexor se hacen necesarios. La siguiente partida corresponde a una torre de comunicaciones sencilla, compuesta por la torre, la antena, el duplexor, el amplificador, el armario para exteriores y la comunicación vía satélite para el acceso a la red externa junto con el equipo necesario para desplegar OpenBTS.

| Elemento | Descripción | Unidades | Precio unitario € | Subtotal € |
|---|---|---|---|---|
| SDR | Software Defined Radio. NI 2922 | 1 | 2.680,00 | 2.680,00 |
| Servidor | Servidor PC compatible con, al menos, una interfaz de red Gigabit Ethernet y procesador de, al menos, 2 núcleos. | 1 | 371,07 | 371,07 |
| UTP cat 6 | Digitus Cable de Red RJ45 UTP Cat.6 10/100/1000 Gris 2m | 1 | 2,44 | 2,44 |
| Tramo torre | Mástil de antena de 1,65 m de alto, para unión por enchufe, fabricado con tubo de acero de 35 mm de diámetro y 1,5 mm de espesor, con tratamiento anticorrosión, incluso accesorios. | 12 | 10,57 | 126,84 |
| Tramo superior | Tramo superior de 2,5 m de alto y sección triangular de 180 mm de lado, para unión por enchufe, fabricado con tubo de acero de 20 mm de diámetro y celosía de acero de 7 mm de espesor, con tratamiento anticorrosión, para formación de torreta de sujeción de antena y accesorios. | 1 | 94,96 | 94,96 |
| Fijación torreta | Placa base rígida, cuadrada, para soldar o atornillar, para fijación de tramo de sección triangular mediante unión por enchufe, incluso accesorios de fijación. | 1 | 13,14 | 13,14 |
| Cable acero | Cable de acero de 2 mm de sección, para grupo de vientos de sujeción de torreta, incluso p/p de placa base, herrajes y tensores. | 39 | 1,11 | 43,29 |
| Duplexor | Duplexor GSM para TX y RX | 1 | 450 | 450 |
| MHA | Amplificador de mástil para GSM. Marca Amphenol Jaybeam, modelo TTA-GLG000H | 1 | 2,44 | 2,44 |
| Antena | Antena para exteriores Omnidireccional. Amphenol-JayBeam. Modelo 7825700 | 1 | 250 | 250 |
| Conexión-Satelite | Reflector parabólico, de acero electrozincado, acabado con pintura poliéster color blanco, de 60 cm de diámetro, ancho de banda de 10,7 a 12,75 GHz. | 1 | 21,34 | 21,34 |
| Armario | Armario para exteriores | 1 | 150 | 150 |
| | | | Total (IVA no incluido): | 3.834,45 |

**174. PRESUPUESTO DE UNAS INSTALACIÓN EN CAMPO**

Si nuestra instalación necesita disponer de más de una estación base, el presupuesto total será: el número de estaciones base requeridas por el coste de la partida torre comunicaciones.

## 5.2 ENSEÑANZA EN LABORATORIO DE COMUNICACIONES.

La principal utilidad de este proyecto ha sido la del desarrollo de un proyecto final de carrera dentro de la titulación de Ingeniero de Telecomunicación. Gracias a él se ha podido estudiar a fondo la interfaz radio Um de forma real, y verificar su funcionamiento mediante la conexión entre MS y BTS. Poder realizar llamadas, enviar SMS y navegar por internet, lo que permite obtener un conocimiento sólido sobre el estándar GSM.

El equipo USRP2 a ser un dispositivo completamente configurable, permite también la posibilidad de diseñar a medida cualquier tipo de comunicación, ya sea digital o analógica dentro de los márgenes de funcionamiento del mismo. Fortalezas principales para su uso en enseñanza:

- El coste total ronda los 3000€. Menor que otro sistemas de similares características.
- Gracias a la conexión GigabitEthernet y un PC potente, el procesado puede ser en tiempo real.
- El software necesario es muy sencillo de instalar y configurar.
- El desarrollo de sistema se hace muy rápido gracias a las características anteriores.

En un entorno de docencia de comunicaciones móviles, las posibilidades del sistema son numerosas:

- Software Defined Radio.
- Cognitive Radio.
- Procesado digital de señales.
- Procesado digital de señales multitasa.
- Sistemas de comunicaciones.
- Diseño e implementación de sistemas con FPGA.
- Y un largo etcétera en múltiples áreas, por ejemplo, sistemas de comunicaciones satélite, radioastronomía, seguimiento de vida salvaje, RFID, sistemas de sónar…

## 5.3 TELEFONÍA EN ZONAS RURALES.

**175. HTTP://WWW.VNL.IN EJEMPLO DE NEGOCIO BASADO EN LAS MICROTELECOM**

Las comunicaciones móviles en zonas rurales y poco pobladas no han sido el principal interés para los operadores de telecomunicaciones, debido principalmente al alto coste de los despliegues y la baja rentabilidad de los mismos, ya que los operadores quieren mantener su ROI (Return of Investment o retorno de la inversión) a unos niveles altos.

Aparece un modelo de negocio llamado Microtelecom, que trata de optimizar la infraestructura de telecomunicaciones para una aplicación muy específica con poca inversión inicial en las zonas rurales a las que los grandes operadores no han llegado. Las características del modelo son: el bajo coste, la facilidad del despliegue, mantenimiento casi nulo y flexibilidad. Esto le permite mantener el beneficio al operador y al usuario del mismo.

Este modelo minimiza el riesgo de los grandes operadores al desplegar sus redes en zonas remotas. El modelo de microtelecom aprovecha las ventajas de OpenBTS para poder hacer frente al desarrollo de la red de telecomunicaciones en zonas rurales. Pudiendo controlar el ROI en poco tiempo. Para el caso de las zonas rurales, el despliegue se realiza en microceldas de poca área de cobertura, proporcionando servicios de voz, SMS e Internet en esas pequeñas celdas. Gracias al

diseño de OpenBTS, no es necesario disponer de multiples servidores Asterisk en la red, ya que con uno solo se puede gestionar las llamadas entre todas las celdas y manteniendo un coste casi cero para aquellas llamadas dentro de la cobertura del proveedor, por ser llamadas VoIP.

Un ejemplo de telefonía en zonas rurales es el proyecto NavegaPará, en el que se ha desplegado una red troncal para cincuenta ciudades de la región de Pará, al norte de Brasil, con la idea de que dispongan de una infraestructura GSM+GPRS basada en el sistema OpenBTS. De esta forma se pretende mejorar su forma de vida al proporcionarle acceso a teléfonos móviles para realizar llamadas de emergencia y las necesidades de comunicación básicas que tengan.

El reto al que se enfrentaban en este proyecto es que los pueblos se encuentran muy dispersos en medio de la selva amazónica, sin acceso, a veces, a electricidad. Que se ha solventado con el programa "Luz para todos" del gobierno de Brasil.

**176. OPENBTS DESPLEGADA EN LA SELVA**

## 5.4 COMUNICACIONES TRAS DESASTRES NATURALES

Los desastres naturales como los terremotos, tsunamis, y grandes tormentas, son circunstancias impredecibles que, entre otros efectos, pueden afectar a los servicios de comunicaciones, llegando a conseguir que fallen por completo. Una vez ha sido destruida la infraestructura móvil, volverla a desplegar supone un coste en presupuesto y tiempo muy elevado para los operadores de telecomunicaciones.

**177. EJEMPLO DE INFRAESTRUCTURA GSM PARA EMERGENCIAS**

Tras un desastre natural, se necesita un despliegue rápido de las comunicaciones, para poder ayudar de forma efectiva a los equipos de emergencias. Hasta ahora se viene haciendo uso de los equipos de radioaficionados en las zonas aisladas, que hacen uso de ciertas frecuencias destinadas en casos de emergencias. Pero estos equipos tienen limitaciones, ya que requieren de personal cualificado para poder utilizarlos, otra de las limitaciones es su ubicación, ya que suelen estar ubicadas en edificios públicos, o viviendas privadas de forma que no es accesible para la gran mayoría de afectados.

Una solución al problema es el proyecto desarrollado en el presente documento, ya que ofrece una infraestructura de red GSM de bajo coste. Con la capacidad de poder ser desplegada en muy poco tiempo ya que tiene muy pocos elementos hardware. Otra de las ventajas de esta solución es que no requiere de personal cualificado para poder usarse una vez desplegada, ya que sólo se necesita de un dispositivo móvil GSM que no requiere de formación.

En el caso de este sistema, se necesitaría de un amplificador de señal, ya que haciendo uso sólo del USRP obtendríamos un alcance de unos 30 metros. La empresa Range Networks ofrece dispositivos preparados con OpenBTS con una potencia configurable como el de la 178. OpenCell Series de Range networks, desde 100mW para test en laboratorio, hasta 50W de potencia de salida con un alcance de hasta 35km y con capacidad de hasta 35 llamadas simultáneas. [15]

**178. OPENCELL SERIES DE RANGE NETWORKS**

# 6. CONCLUSIONES Y TRABAJO FUTURO

El presente documento ilustra el despliegue de una red de telefonía móvil basado en el estándar 2G GSM mediante el uso de un equipo SDR.

Está enfocado a su aplicación didáctica en la enseñanza, ya que permite comprender los conceptos asociados a una red de telefonía, desde el canal físico y el análisis de multitud de parámetros implicados en el espectro, hasta el estudio del protocolo SIP y RTP y los mensajes que se intercambian los diferentes elementos que componen la arquitectura de una red VoIP actual.

A modo de resumen se van a enumerar las lecciones aprendidas gracias al desarrollo del proyecto:

- Modulación y constelación GMSK. Espectro de la misma.
- Codificación del canal en GSM.
- Uso eficiente del espectro con la combinación FDD/FDMA/TDMA para que múltiples usuarios puedan comunicarse de forma simultánea.
- Estudio de los canales lógicos de GSM, tanto los de control por parte de la BTS, como los de señalización y tráfico del abonado.
- Estudio del intercambio de mensajes SIP en una red VoIP.
- Configuración de un plan de llamadas para una centralita VoIP Asterisk.
- Contratación de un servicio troncal SIP para la realización de llamadas fuera de la red privada.

Como siguientes pasos para continuar la línea del estudio de las redes celulares se han identificado las siguientes ramas:

- Desplegar más de una celda GSM y ver uno de los mecanismos más importantes en las redes celulares, como es el traspaso de una llamada que esté en curso. Para ello será necesario: el uso de varios equipos SDR; configurar la potencia en ambos equipos para que tengan un área de cobertura común pequeño; configurar los diferentes elementos de la red, OpenBTS y Asterisk, para poder realizar el traspaso de llamadas correctamente.
- La otra posibilidad es la evolución del sistema GSM+GPRS a la tercera generación de comunicaciones móviles, 3G o UMTS. Para ello el proyecto OpenBTS dispone de una versión del sistema OpenBTS para 3G que todavía está en fase de pruebas. Este paso nos permitiría estudiar en profundidad una red más actual a la GSM pero con funcionalidades similares.

# ANEXO 1. INSTALACIÓN DEL EQUIPO SDR EN EL SERVIDOR

El dispositivo SDR utilizado, NI 2922, se comunica mediante un puerto Gigabit Ethernet. Lo primero que deberemos configurar será dicha tarjeta Gigabit Ethernet en nuestro servidor. Para ello, editamos el archivo /etc/network/interfaces para añadir o modificar la entrada correspondiente a la interfaz de red a la que está conectado el equipo SDR.

```
1. sudo nano /etc/network/interfaces
2. # La interfaz secundaria
   auto eth0
   iface eth0 inet static
          address 192.168.10.11
          netmask 255.255.255.0
```

En nuestro caso `eth0` es la interfaz a la que está conectado.

Ahora procederemos a instalar los requisitos previos para los *drivers* del dispositivo.

```
sudo apt-get install python libboost-all-dev libusb-1.0-0-dev
```

Descargamos el *driver* de la web de Ettus, ya que es equivalente al producto de National Instruments:

```
wget http://files.ettus.com/binaries/uhd_stable/uhd_003.004.002-release/uhd_003.004.002-release_Ubuntu-12.04-i686.deb
sudo dpkg -i uhd_003.004.002-release_Ubuntu-12.04-i686.deb
```

Una vez instalado el *driver*, comprobamos que funciona y encuentra el elemento SDR:

```
openbts@OpenBTS:~$ uhd_find_devices
linux; GNU C++ version 4.6.3; Boost_104601; UHD_003.004.002-release

--------------------------------------------------
-- UHD Device 0
--------------------------------------------------
Device Address:
    type: usrp2
    addr: 192.168.10.2
    name:
    serial: F43776

openbts@OpenBTS:~$ uhd_usrp_probe
linux; GNU C++ version 4.6.3; Boost_104601; UHD_003.004.002-release

-- Opening a USRP2/N-Series device...
-- Current recv frame size: 1472 bytes
-- Current send frame size: 1472 bytes

UHD Warning:
    The recv buffer could not be resized sufficiently.
    Target sock buff size: 50000000 bytes.
    Actual sock buff size: 163840 bytes.
    See the transport application notes on buffer resizing.
    Please run: sudo sysctl -w net.core.rmem_max=50000000

UHD Warning:
    The recv buffer could not be resized sufficiently.
    Target sock buff size: 50000000 bytes.
    Actual sock buff size: 163840 bytes.
    See the transport application notes on buffer resizing.
    Please run: sudo sysctl -w net.core.rmem_max=50000000
```

```
UHD Warning:
    The send buffer could not be resized sufficiently.
    Target sock buff size: 1048576 bytes.
    Actual sock buff size: 163840 bytes.
    See the transport application notes on buffer resizing.
    Please run: sudo sysctl -w net.core.wmem_max=1048576

UHD Warning:
    Unable to set the thread priority. Performance may be negatively affected.
    Please see the general application notes in the manual for instructions.
    EnvironmentError: OSError: error in pthread_setschedparam
  ____________________________________________________
 /
|       Device: USRP2 / N-Series Device
|     ________________________________________________
|    /
|   |       Mboard: USRP-N210-REV4
|   |   hardware: 2577
|   |   product: 30194
|   |   mac-addr: 00:80:2f:0a:de:bc
|   |   ip-addr: 192.168.10.2
|   |   gpsdo: none
|   |   serial: F43776
|   |
|   |   Time sources: none, external, _external_, mimo
|   |   Clock sources: internal, external, mimo
|   |   Sensors: mimo_locked, ref_locked
|   |     ____________________________________________________
|   |    /
|   |   |       RX DSP: 0
|   |   |   Freq range: -50.000 to 50.000 Mhz
|   |     ____________________________________________________
```

Al leer el resumen de la configuración del equipo, se observan unas advertencias:

```
The recv buffer could not be resized sufficiently
The send buffer could not be resized sufficiently.
Unable to set the thread priority
```

Y nos recomiendan cómo solventarlas:

```
Please run: sudo sysctl -w net.core.rmem_max=50000000
Please run: sudo sysctl -w net.core.wmem_max=1048576
```

Por lo que hacemos caso a la recomendación y ejecutamos esos comandos para modificar los tamaños de los *buffers* de recepción y transmisión. Para no tener que configurar esto cada vez que encendemos el servidor, los añadimos al archivo /etc/rc.local:

```
#!/bin/sh -e
#
# rc.local
#
# This script is executed at the end of each multiuser runlevel.
# Make sure that the script will "exit 0" on success or any other
# value on error.
#
# In order to enable or disable this script just change the execution
# bits.
#
# By default this script does nothing.

# Fijamos los valores para el driver UHD
```

```
sudo sysctl -w net.core.rmem_max=50000000
sudo sysctl -w net.core.wmem_max=1048576

exit 0
```

Y también modificar el fichero /etc/security/limits.conf para evitar los problemas del ajuste de la prioridad:

```
# /etc/security/limits.conf
#
#Each line describes a limit for a user in the form:
#
#<domain>        <type>  <item>  <value>
#
#Where:
#<domain> can be:
#        - an user name
#        - a group name, with @group syntax
#        - the wildcard *, for default entry
#        - the wildcard %, can be also used with %group syntax,
#                 for maxlogin limit
#        - NOTE: group and wildcard limits are not applied to root.
#          To apply a limit to the root user, <domain> must be
#          the literal username root.
#
#<type> can have the two values:
#        - "soft" for enforcing the soft limits
#        - "hard" for enforcing hard limits
#
#<item> can be one of the following:
#        - core - limits the core file size (KB)
#        - data - max data size (KB)
#        - fsize - maximum filesize (KB)
#        - memlock - max locked-in-memory address space (KB)
#        - nofile - max number of open files
#        - rss - max resident set size (KB)
#        - stack - max stack size (KB)
#        - cpu - max CPU time (MIN)
#        - nproc - max number of processes
#        - as - address space limit (KB)
#        - maxlogins - max number of logins for this user
#        - maxsyslogins - max number of logins on the system
#        - priority - the priority to run user process with
#        - locks - max number of file locks the user can hold
#        - sigpending - max number of pending signals
#        - msgqueue - max memory used by POSIX message queues (bytes)
#        - nice - max nice priority allowed to raise to values: [-20, 19]
#        - rtprio - max realtime priority
#        - chroot - change root to directory (Debian-specific)
#
#<domain>      <type>  <item>         <value>
#

@openbts        -       rtprio          99

#*               soft    core            0
#root            hard    core            100000
#*               hard    rss             10000
#@student        hard    nproc           20
#@faculty        soft    nproc           20
#@faculty        hard    nproc           50
#ftp             hard    nproc           0
#ftp             -       chroot          /ftp
#@student        -       maxlogins       4

# End of file
```

Con esto finalmente tenemos correctamente configurado el driver UHD, y la salida completa del comando "`uhd_usrp_probe`" es:

```
openbts@OpenBTS:~$ uhd_usrp_probe
linux; GNU C++ version 4.6.3; Boost_104601; UHD_003.004.002-release

-- Opening a USRP2/N-Series device...
-- Current recv frame size: 1472 bytes
-- Current send frame size: 1472 bytes
  _____________________________________________________
 /
|       Device: USRP2 / N-Series Device
|     _____________________________________________________
|    /
|    |       Mboard: USRP-N210-REV4
|    |   hardware: 2577
|    |   product: 30194
|    |   mac-addr: 00:80:2f:0a:de:bc
|    |   ip-addr: 192.168.10.2
|    |   gpsdo: none
|    |   serial: F43776
|    |
|    |   Time sources: none, external, _external_, mimo
|    |   Clock sources: internal, external, mimo
|    |   Sensors: mimo_locked, ref_locked
|    |     _____________________________________________________
|    |    /
|    |    |       RX DSP: 0
|    |    |   Freq range: -50.000 to 50.000 Mhz
|    |
|    |     _____________________________________________________
|    |    /
|    |    |       RX DSP: 1
|    |    |   Freq range: -50.000 to 50.000 Mhz
|    |
|    |     _____________________________________________________
|    |    /
|    |    |       RX Dboard: A
|    |    |   ID: WBX v3, WBX v3 + Simple GDB (0x0057)
|    |    |   Serial: F41910
|    |    |     _____________________________________________________
|    |    |    /
|    |    |    |       RX Subdev: 0
|    |    |    |   Name: WBX RX v3 + Simple GDB
|    |    |    |   Antennas: TX/RX, RX2, CAL
|    |    |    |   Sensors: lo_locked
|    |    |    |   Freq range: 68.750 to 2200.000 Mhz
|    |    |    |   Gain range PGA0: 0.0 to 31.5 step 0.5 dB
|    |    |    |   Connection Type: IQ
|    |    |    |   Uses LO offset: No
|    |    |    |     _____________________________________________________
|    |    |    |    /
|    |    |    |    |       RX Codec: A
|    |    |    |    |   Name: ads62p44
|    |    |    |    |   Gain range digital: 0.0 to 6.0 step 0.5 dB
|    |    |    |    |   Gain range fine: 0.0 to 0.5 step 0.1 dB
|    |    |
|    |    |     _____________________________________________________
|    |    |    /
|    |    |    |       TX DSP: 0
|    |    |    |   Freq range: -250.000 to 250.000 Mhz
|    |    |
|    |    |     _____________________________________________________
|    |    |    /
|    |    |    |       TX Dboard: A
|    |    |    |   ID: WBX v3 (0x0056)
|    |    |    |   Serial: F41910
|    |    |    |   ID: WBX + Simple GDB, WBX v3 + Simple GDB, WBX v4 + Simple GDB
(0x004f)
|    |    |    |   Serial: F400EB
|    |    |    |     _____________________________________________________
```

```
|   |   |    /
|   |   |   |       TX Subdev: 0
|   |   |   |   Name: WBX TX v3 + Simple GDB
|   |   |   |   Antennas: TX/RX, CAL
|   |   |   |   Sensors: lo_locked
|   |   |   |   Freq range: 68.750 to 2200.000 Mhz
|   |   |   |   Gain range PGA0: 0.0 to 31.0 step 1.0 dB
|   |   |   |   Connection Type: IQ
|   |   |   |   Uses LO offset: No
|   |   |    ____________________________________________________________
|   |   |    /
|   |   |   |       TX Codec: A
|   |   |   |   Name: ad9777
|   |   |   |   Gain Elements: None
```

Con todo esto ya disponemos del equipo SDR correctamente configurado para ser utilizado con OpenBTS.

# ANEXO 2. INSTALACIÓN Y CONFIGURACIÓN DE OPENBTS

La instalación y configuración del paquete OpenBTS previo a la versión 5.0 era bastante tedioso, ya que se tenía que configurar todo por separado y era muy fácil cometer algún fallo. Con la versión 5.0 esto es mucho más sencillo gracias a uno de los paquetes incluidos que se encarga de realizar todo el proceso de configuración de forma automática. Para hacer las cosas más sencillas aún, el 12 de enero de 2015 uno de los impulsores del proyecto publicó un libro de forma gratuita donde describe todo el proceso de instalación, configuración y ajustes de rendimiento para poder sacarle el mejor partido al sistema. Aquí simplemente realizaremos un breve resumen con lo imprescindible y algunas notas que no aparecen en el libro y son necesarias.

## COMENZAREMOS POR INSTALAR GIT.

Necesitamos una versión superior a la 1.8.2, pero si utilizamos el servidor Ubuntu 12.04 y los repositorios que trae por defecto, al intentar una instalación por medio de apt-get nos dirá que ya está en su versión más reciente que resulta ser la 1.7. Seguiremos los siguientes pasos para tener la versión más actualizada:

Añadimos el repositorio oficial de GIT

```
sudo add-apt-repository ppa:git-core/ppa
```

Actualizamos la base da datos de paquetes

```
sudo apt-get update
```

Instalamos la última versión de GIT

```
sudo apt-get install git
```

Comprobamos la versión que tenemos:

```
git --version
```

Obtenemos en nuestro caso:

```
git version 2.3.0
```

Una vez que disponemos de una versión de GIT superior a la 1.8.2 podemos comenzar la descarga, compilación e instalación del paquete OpenBTS.

## INSTALACIÓN DE OPENBTS.

Descarga:

```
git clone https://github.com/RangeNetworks/dev.git
cd dev
./clone.sh
./switchto.sh 5.0
```

Tras estos pasos tendremos el código fuente de la versión 5.0 de OpenBTS.

Compilación:

```
./build.sh N210
```

Con el argumento N210 le hemos indicado que el transceptor a compilar será el correspondiente al equipo de la casa ETTUS, N210. Este equipo SDR es totalmente compatible con el utilizado en nuestro caso, el NI 2922.

Instalación:

```
cd dev/BUILDS/tiempo_compilacion/
```

Donde el directorio `tiempo_compilación` será el correspondiente al momento de la compilación anterior.

Añadimos un repositorio e instalamos:

```
sudo add-apt-repository ppa:chris-lea/zeromq
sudo apt-get update
sudo dkpg –i libcoredumper1_1.2.1-1_i386.deb
sudo dpkg –i liba53_0.1_i386.deb
sudo dpkg –i range-configs_5.0_all.deb
sudo dkpg –i range-asterisk*.deb
sudo dpkg –i sipauthserve_5.0_i386.deb
sudo dpkg –i smqueue_5.0_i386.deb
sudo dpkg –i openbts_5.0_i386.deb
```

Tras esto tendremos en la carpeta /OpenBTS/ todos los programas referidos al paquete OpenBTS. Se han configurado también como servicios del sistema, por lo que al inicio del equipo se ejecutarán todos de forma automática.

## CONFIGURACIÓN DE OPENBTS.

Para configurar todos los parámetros del sistema, OpenBTS dispone de un terminal cliente en el que podremos ver y modificar todas las características que necesitemos.

Para entrar en el cliente ejecutamos:

```
sudo ./OpenBTS/OpenBTSCLI
```

Y obtendremos un terminal de la forma:

Una referencia para el uso de esta línea de comandos la podremos encontrar en los apéndices B y C del manual de usuario de OpenBTS.

# ANEXO 3. INSTALACIÓN DE OSMOCOM-BB

OsmocomBB es un conjunto de aplicaciones para el estudio de telefonía GSM. Toda la información necesaria se puede obtener de su dirección web:

http://bb.osmocom.org/trac/

Las aplicaciones más interesantes son las siguientes:

1. *Mobile+Layer1*: Estas dos aplicaciones en conjunto son capaces de funcionar como un teléfono móvil GSM convencional.
    a. *Layer1* es el firmware que se instala en la RAM de un teléfono móvil y actúa cómo la capa 1 de la pila de protocolos GSM.
    b. *Mobile* es el software que se ejecuta en un PC y hace las veces de capas 2 y 3 en la pila de protocolos GSM. Dispone de una interfaz de comandos para poder gestionar el teléfono.
2. RSSI: Firmware que se carga en la RAM de un teléfono móvil de forma que dicho teléfono tiene la funcionalidad de analizar los diferentes ARFCN de las bandas de 900 y 1800 MHz de GSM. Permite medir la potencia de la señal recibida, obtener cierta información de la celda y ver la potencia de cada time slot.
3. EMI: Este firmware requiere modificar la electrónica del teléfono móvil para eliminar un filtro de RF que hay antes de la antena del mismo, de tal forma que el móvil tenga la capacidad de emitir en toda la banda GSM, tanto en el enlace de subida, como de bajada. Una vez disponemos del móvil con dicha modificación podremos cargar este firmware en la RAM. La principal utilidad del firmware es la de emitir "ruido" en diferentes *time slots* del canal elegido y con la potencia elegida. De esta forma podremos poner a prueba nuestro enlace ante emisiones de ruido espontáneas. ATENCIÓN: Al emitir ruido en estas bandas estamos dejando sin servicio la estación base en cuestión, con las consecuencias legales que ello pueda acarrear.
4. *Transceiver+TRX*: *TRX* es un firmware que pretende convertir el teléfono móvil en un transceptor para una estación base. Junto con OpenBTS y el software *transceiver* de OsmocomBB se podría montar una estación base con un único ARFCN. El teléfono móvil necesita la misma modificación electrónica que para el firmware EMI.

## HARDWARE

Una vez conocidas las capacidades de este software, se ha preparado la parte hardware. En este caso se ha utilizado un teléfono móvil cuyo procesador esté basado en el que recomiendan en su web, concretamente en el chip de Texas Instruments Calypso. El modelo seleccionado es un Motorola C123 junto con un cable adaptador de puerto serie a USB basado en el chip FT232.

Como se quiere poder utilizar todas las funcionalidades del software, necesitamos modificar el teléfono para poder emitir en la banda del enlace descendente. Para ello se ha retirado el filtro como recomiendan en la web del proyecto.

Una vez preparada toda la parte hardware, comenzaremos la instalación de OsmocomBB.

## SOFTWARE

Para su instalación, seguiremos las pautas indicadas en la web principal como se comentó anteriormente. Aquí resumiremos los pasos a seguir y algunas notas aclaratorias que no aparecen en la web y son necesarias.

Comenzaremos por instalar las dependencias necesarias para compilar el software. En rojo están aquellos paquetes que son necesarios y no aparecen en la web:

```
sudo apt-get install libtool shtool automake autoconf git-core pkg-config make
gcc libpcsclite libfftw3-dev
```

Otra de la dependencia necesaria es la librería `libosmocom` que deberemos de descargar y compilar:

```
git clone git://git.osmocom.org/libosmocore.git
cd libosmocore/
autoreconf -i
./configure
make
sudo make install
cd ..
```

También la librería `libosmo-dsp` es necesaria:

```
git clone git://git.osmocom.org/libosmo-dsp.git
cd libosmo-dsp
autoconf -i
./configure --prefix=/usr/
make
sudo make install
cd ..
```

El siguiente paso es disponer de un compilador para ARM, ya que la parte del firmware se va a ejecutar en el procesador móvil y es un ARMv7. En este caso recomiendan instalar `GNUArmToolchain`:

Instalamos las dependencias del compilador:

```
sudo apt-get install build-essential libgmp3-dev libmpfr-dev libx11-6 libx11-
dev texinfo flex bison libncurses5 libncurses5-dbg libncurses5-dev
libncursesw5 libncursesw5-dbg libncursesw5-dev zlibc zlib1g-dev libmpfr4
libmpc-dev
```

Creamos un directorio para el *toolchain*:

```
mkdir toolchain
```

Descargamos un script para instalar el compilador:

```
cd toolchain
wget http://bb.osmocom.org/trac/raw-attachment/wiki/GnuArmToolchain/gnu-arm-
build.2.sh
```

Le damos permisos de ejecución:

```
chmod +x gnu-arm-build.2.sh
```

En el directorio donde se ha descargado el script, creamos los siguientes subdirectorios:

```
mkdir build install src
```

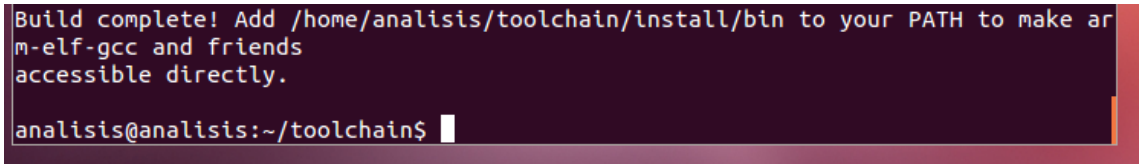
Descargamos el código fuente del compilador en la carpeta src:

```
cd src/
wget http://ftp.gnu.org/gnu/gcc/gcc-4.5.2/gcc-4.5.2.tar.bz2
wget http://ftp.gnu.org/gnu/binutils/binutils-2.21.1a.tar.bz2
wget ftp://sources.redhat.com/pub/newlib/newlib-1.19.0.tar.gz
```

Y finalmente ejecutamos el script para compilar `GNUArmToolchain`:

```
cd ..
./gnu-arm-build.2.sh
```

Tras un tiempo (25-40 minutos dependiendo de la máquina en el que se esté ejecutando) aparecerá el siguiente mensaje indicando que ha terminado correctamente:




**179. COMPILACIÓN COMPLETADA**

Una vez esté instalado, añadiremos el directorio /bin generado por la compilación a la variable del sistema `$PATH`. Puesto que estamos utilizando Ubuntu como distribución, con BASH como intérprete de comandos, editamos el archivo "~/.bashrc" y añadimos la siguiente línea al final del archivo:

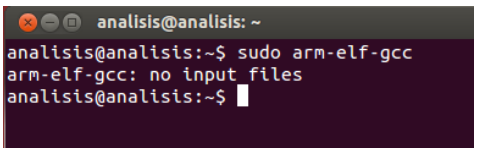
```
export PATH=$PATH:/home/analisis/toolchain/install/bin
```

Según la web ya estaríamos en condiciones de compilar OsmocomBB, pero se les ha olvidado comentar que tenemos que añadir al PATH también cuando trabajamos como superusuario, ya que para el superusuario no está ese directorio en su PATH y por lo tanto obtendríamos un error al compilar OsmocomBB.

Como solución, hay que añadir a la línea `secure_path` del archivo /etc/sudoers la ruta donde está el directorio bin del compilador de ARM:

```
Defaults secure_path=":/home/analisis/toolchain/install/bin"
```

Para comprobar que está bien configurado, ejecutamos por ejemplo el compilador GCC para ARM:




**180. COMPILADOR ARM DISPONIBLE**

Si obtenemos ese resultado es que está bien configurado el equipo para proceder a la compilación de OsmocomBB.

Comenzamos ya la instalación de OsmocomBB, empezando por obtener el código fuente:

```
git clone git://git.osmocom.org/osmocom-bb.git
```

```
cd osmocom-bb
```

Puesto que vamos a utilizar funcionalidades para poder emitir con nuestro teléfono, cambiamos en GIT a la rama de test:

```
git checkout -b testing remotes/origin/sylvain/testing
```

Una vez descargados los archivos fuente, necesitamos modificar el archivo Makefile referente a la compilación del firmware para poder tener soporte de transmisión, ya que por defecto esta deshabilitado. Editamos el archivo osmocom-bb/src/target/firmware/Makefile y quitamos el comentario a la línea que habilita la transmisión, quedando de la forma:

```
#
# Build options
#

# Uncomment this line if you want to enable Tx (Transmit) Support.
CFLAGS += -DCONFIG_TX_ENABLE
```

**181. LINEA A MODIFICAR PARA PERMITIR LA TRANSMISIÓN**

Ya podemos compilar el sistema OsmocomBB con soporte para transmisión y habilitando que se compile también el software *transceiver*.

```
cd src
make HOST_layer23_CONFARGS=--enable-transceiver
```

Tras todo esto dispondremos del sistema OsmocomBB casi al completo. El firmware EMI está en una rama diferente en el repositorio GIT de OsmocomBB. Para poder disponer de él, crearemos una nueva carpeta en nuestro directorio:

```
mkdir emi
```

En ella obtendremos la rama GIT que incluye dicho firmware:

```
cd emi
git init
git remote add -t jolly/emi -f origin git://git.osmocom.org/osmocom-bb.git
git checkout jolly/emi
```

De nuevo modificamos el archivo emi/osmocom-bb/src/target/firmware/Makefile para dar soporte a la transmisión. Tras la modificación ejecutamos:

```
cd src
make
```

Tras todo esto tendremos en diferentes directorios los firmwares a cargar en el móvil, la aplicación necesaria para cargar dichos firmwares y las aplicaciones cliente. Para facilitar todo el trabajo se han definido diferentes scripts que ejecutaremos en función de nuestras necesidades. Comenzaremos por los dos más sencillos, que no necesitan de un cliente en el PC, los firmware RSSI y EMI.

Script de carga del firmware RSSI en el móvil, rssi.sh:

```
#!/bin/bash
# -*- ENCODING: UTF-8 -*-
./osmocom-bb/src/host/osmocon/osmocon -p /dev/ttyUSB0 -m c123xor -c ./osmocom-
bb/src/target/firmware/board/compal_e88/rssi.highram.bin            ./osmocom-
bb/src/target/firmware/board/compal_e88/chainload.compalram.bin
```

Script de carga del firmware EMI en el móvil, emi.sh:

```
#!/bin/bash
# -*- ENCODING: UTF-8 -*-
./emi/src/host/osmocon/osmocon    -p    /dev/ttyUSB0    -m    c123xor    -c
./emi/src/target/firmware/board/compal_e88/emi.highram.bin
./emi/src/target/firmware/board/compal_e88/chainload.compalram.bin
```

Para el conjunto *Mobile+Layer1* necesitamos trabajar con 3 terminales, uno con el monitor de eventos del firmware al ejecutar la carga de éste en el móvil, otro con el monitor de eventos del móvil, y un último terminal en el que nos conectaremos mediante telnet al móvil y podremos operar con él.

Script de carga de firmware layer1.sh:

```
#!/bin/bash
# -*- ENCODING: UTF-8 -*-
./osmocom-bb/src/host/osmocon/osmocon -p /dev/ttyUSB0   -m c123xor osmocom-
bb/src/target/firmware/board/compal_e88/layer1.compalram.bin
```

Antes de poner a funcionar la aplicación *mobile* hay que crear un archivo de configuración vacío:

```
mkdir .osmocom
cd .osmocom
mkdir bb
cd bb
nano mobile.cfg
```

Guardamos el archivo vacío.

```
touch /home/analisis/.osmocom/bb/mobile.cfg
```

Script de inicio de la aplicación mobile.sh:

```
#!/bin/bash
# -*- ENCODING: UTF-8 -*-
./osmocom-bb/src/host/layer23/src/mobile/mobile -i 127.0.0.1
```

Finalmente nos conectamos al móvil para poder operar con él:

```
telenet localhost 4247
```

Tras todo esto dispondremos de un móvil por software completamente configurable.

# ANEXO 4. OBTENCIÓN DEL IMSI DE UNA TARJETA SIM

El número IMSI de una tarjeta SIM es necesario para OpenBTS, ya que los usuarios dentro de la base de datos son de la forma IMSIXXXXXXXXXXXXXXX. De esta forma podremos identificar de forma única a cada usuario móvil en la red GSM. Para poder obtenerlo hay varias formas, y aquí comentaremos dos de ellas muy sencillas.

La primera opción requiere de OpenBTS+SDR funcionando. Configuraremos OpenBTS para que todos los móviles que lo intenten puedan conectarse a la red. Una vez conectados a la red, el usuario podrá enviar un SMS al número 411 y la red le responderá con un SMS con el IMSI así como el texto enviado previamente el usuario.

Dentro de OpenBTS configuramos el registro para abrir la red a todos:

```
OpenBTS> config Control.LUR.OpenRegistration .*
```

Tras abrir el registro, nos conectaremos a la red GSM con el móvil, enviaremos un SMS al 411 y esperaremos la respuesta con el IMSI.

Para después volver a cerrar el registro a todos los dispositivos móviles que no estén en la base de datos de dispositivos autorizados, ejecutamos:

```
OpenBTS> unconfig Control.LUR.OpenRegistration .*
```

La segunda opción para obtener el IMSI es utilizar el software Osmocom-BB descrito en el anexo anterior. Una vez configurado, y con la tarjeta SIM de la que queremos obtener dicho código, podremos realizar un análisis de la misma desde el terminal. A continuación mostramos el resultado de leer toda la información contenida por las SIMs utilizadas para el proyecto.

Pasos para obtener la información con OsmocomBB:

1. `OsmocomBB> enable`
2. `OsmocomBB# show subscriber`

Resultados obtenidos con las diferentes tarjetas SIM:

Con la tarjeta SIM china:

```
IMSI: 460011901250000
ICCID: 982196000000027105
SMS Service Center Address: +8613010112500
Status: U1_UPDATED  IMSI detached
LAI: MCC 001  MNC 01  LAC 0x03e8  (Test, Test)
Key: sequence 0  44 5d c8 a1 5b 9e 94 00
Registered PLMN: MCC 001  MNC 01  (Test, Test)
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
-------+-------
525    |01        (Singapore, SingTel)
525    |02        (Singapore, SingTel-G18)
515    |02        (Philippines, Globe)
520    |01        (Thailand, AIS)
505    |02        (Australia, Optus)
404    |10        (India, AirTel)
404    |31        (India, AirTel)
List of forbidden PLMNs:
MCC    |MNC    |cause
```

```
-------+-------+-------
214    |04     |#255        (Spain, Yoigo)
```

Tarjeta SIM del operador Simyo:

```
IMSI: 214190180058966
ICCID: 8934190014090539662
Service Provider Name: simyo
SMS Service Center Address: +34644109030
Status: U1_UPDATED  IMSI detached
LAI: MCC 001  MNC 01  LAC 0x03e8  (Test, Test)
Key: sequence 0  a3 55 b3 7c 3e 49 eb 97
Registered PLMN: MCC 001  MNC 01  (Test, Test)
Access barred cells: no
Access classes: C6
List of preferred PLMNs:
MCC    |MNC
-------+-------
206    |20        (Belgium, BASE)
262    |03        (Germany, E-Plus)
234    |10        (Guernsey, O2)
208    |20        (France, Bouygues)
204    |08        (Netherlands, KPN)
222    |88        (Italy, Wind)
232    |05        (Austria, Orange)
228    |01        (Switzerland, Swisscom)
202    |01        (Greece, Cosmote)
238    |02        (Denmark, Sonofon / Telenor)
272    |02        (Ireland, O2)
270    |77        (Luxembourg, Tango)
268    |06        (Portugal, TMN)
262    |01        (Germany, T-Mobile)
230    |02        (Czech Republic, O2)
208    |01        (France, Orange)
425    |02        (Israel, Cellcom)
286    |01        (Turkey, Turkcell)
206    |01        (Belgium, Proximus)
240    |01        (Sweden, Telia)
310    |410       (United States of America, Cingular Wireless)
260    |02        (Poland, Era)
216    |01        (Hungary, Pannon GSM)
244    |91        (Finland, Sonera)
```

Tarjeta SIM de Vodafone:

```
IMSI: 214014502081381
ICCID: 8934564521000426259
SMS Service Center Address: +34607003110
Status: U1_UPDATED  IMSI detached
LAI: MCC 001  MNC 01  LAC 0x03e8  (Test, Test)
Key: sequence 0  e7 ec 0a 75 84 3c 58 00
Registered PLMN: MCC 001  MNC 01  (Test, Test)
Access barred cells: no
Access classes: C1
List of preferred PLMNs:
MCC    |MNC
-------+-------
234    |15        (Guernsey, Vodafone)
262    |02        (Germany, Vodafone)
222    |10        (Italy, Vodafone)
230    |03        (Czech Republic, Vodafone)
226    |01        (Romania, Vodafone)
208    |10        (France, SFR)
286    |02        (Turkey, Vodafone)
310    |410       (United States of America, Cingular Wireless)
```

```
250    |01        (Russian Federation, MTS)
202    |05        (Greece, Vodafone)
505    |03        (Australia, Vodafone)
274    |02        (Iceland, P/F Kall)
404    |20        (India, Vodafone IN)
240    |08        (Sweden, Telenor)
272    |01        (Ireland, Vodafone)
242    |01        (Norway, Telenor)
204    |04        (Netherlands, Vodafone)
228    |01        (Switzerland, Swisscom)
404    |11        (India, Vodafone IN)
404    |27        (India, Vodafone IN)
404    |05        (India, Vodafone IN)
216    |70        (Hungary, Vodafone)
604    |00        (Morocco, Moditel)
268    |01        (Portugal, Vodafone)
460    |00        (China, China Mobile)
655    |01        (South Africa, Vodacom)
231    |02        (Slovakia, T-Mobile)
232    |01        (Austria, A1)
724    |03        (Brazil, TIM)
602    |02        (Egypt, Vodafone)
255    |01        (Ukraine, MTS)
278    |01        (Malta, Vodafone)
244    |05        (Finland, Elisa)
260    |01        (Poland, Plus)
334    |03        (Mexico, movistar)
420    |01        (Saudi Arabia, Al Jawal)
730    |01        (Chile, Entel)
293    |40        (Slovenia, Si.mobil)
525    |03        (Singapore, M1)
425    |01        (Israel, Orange)
246    |02        (Lithuania, BITE)
454    |06        (Hong Kong, SmarTone-Vodafone)
248    |02        (Estonia, RLE / Elisa)
219    |10        (Croatia, VIPnet)
238    |01        (Denmark, TDC)
247    |05        (Latvia, Bite)
270    |01        (Luxembourg, LuxGSM)
284    |01        (Bulgaria, M-Tel)
206    |01        (Belgium, Proximus)
220    |01        (Serbia, Telenor)
List of forbidden PLMNs:
MCC    |MNC    |cause
-------+-------+-------
214    |07     |#255        (Spain, movistar)
214    |03     |#255        (Spain, Orange)
214    |04     |#255        (Spain, Yoigo)
```

Tarjeta MicroSIM de Simyo:

```
IMSI: 214190180026482
ICCID: 8934190014090214829
Service Provider Name: simyo
SMS Service Center Address: +34644109030
Status: U1_UPDATED  IMSI detached
LAI: MCC 001  MNC 01  LAC 0x03e8  (Test, Test)
Key: sequence 0  4b 62 d0 6e ae 3b 49 b4
Registered PLMN: MCC 001  MNC 01  (Test, Test)
Access barred cells: no
Access classes: C2
List of preferred PLMNs:
MCC    |MNC
-------+-------
206    |20        (Belgium, BASE)
262    |03        (Germany, E-Plus)
234    |10        (Guernsey, O2)
```

```
208    |20        (France, Bouygues)
204    |08        (Netherlands, KPN)
222    |88        (Italy, Wind)
232    |05        (Austria, Orange)
228    |01        (Switzerland, Swisscom)
202    |01        (Greece, Cosmote)
238    |02        (Denmark, Sonofon / Telenor)
272    |02        (Ireland, O2)
270    |77        (Luxembourg, Tango)
268    |06        (Portugal, TMN)
262    |01        (Germany, T-Mobile)
230    |02        (Czech Republic, O2)
208    |01        (France, Orange)
425    |02        (Israel, Cellcom)
286    |01        (Turkey, Turkcell)
206    |01        (Belgium, Proximus)
240    |01        (Sweden, Telia)
310    |410       (United States of America, Cingular Wireless)
260    |02        (Poland, Era)
216    |01        (Hungary, Pannon GSM)
244    |91        (Finland, Sonera)
```

Como se puede comprobar, este segundo método es mucho más interesante ya que obtenemos muchísima más información de la tarjeta SIM en cuestión. Como contrapartida, con este método necesitamos disponer físicamente de la tarjeta SIM mientras que, con la primera opción, simplemente el usuario de la red nos comunica su IMSI y de esta forma podremos darle de alta en la red sin necesidad de tener físicamente la tarjeta.

# ANEXO 5. LEGISLACIÓN DE EMISIONES RADIOELÉCTRICAS EN ESPAÑA

El aumento de las necesidades de telefonía móvil ha supuesto un aumento de la exposición a las emisiones radioeléctricas. Para tener mayor control sobre dichas emisiones, se aprobó el Real Decreto 1066/2001 que determina las condiciones de protección del dominio público radioeléctrico, restricciones a las emisiones radioeléctricas y medidas de protección sanitaria frente a las emisiones radioeléctricas. También la Orden CTE/23/2002 establece las condiciones para certificaciones de emisiones radioeléctricas y la comprobación de que las emisiones son conformes a los límites establecidos.

Para el caso de este proyecto, hay que centrarse en la banda GSM900 o DCS1800. Esta banda se corresponde a lo que se llama una radiación no ionizante, que es aquella cuya energía no sobrepasa el umbral para ionizar la materia y, por lo tanto, no afectan a la estructura de la materia.

Según el artículo 44 de la Ley 32/2003, General de Telecomunicaciones, el procedimiento de determinación, control e inspección de los niveles de emisión radioeléctrica es facultad del Estado.

Los límites para la exposición a campos electromagnéticos se establecen en dos grupos:

- Exposición controlada u ocupacional: Para aquellos sujetos que son conscientes de la exposición y pueden tomar las medidas de seguridad oportunas. Factor 10 de seguridad en los niveles de referencia.
- Exposición no controlada: Para el público en general, ya que éste no tiene control sobre dicha exposición. Factor 50 de seguridad en los niveles de referencia.

Para las radiaciones hay dos tipos de restricciones:

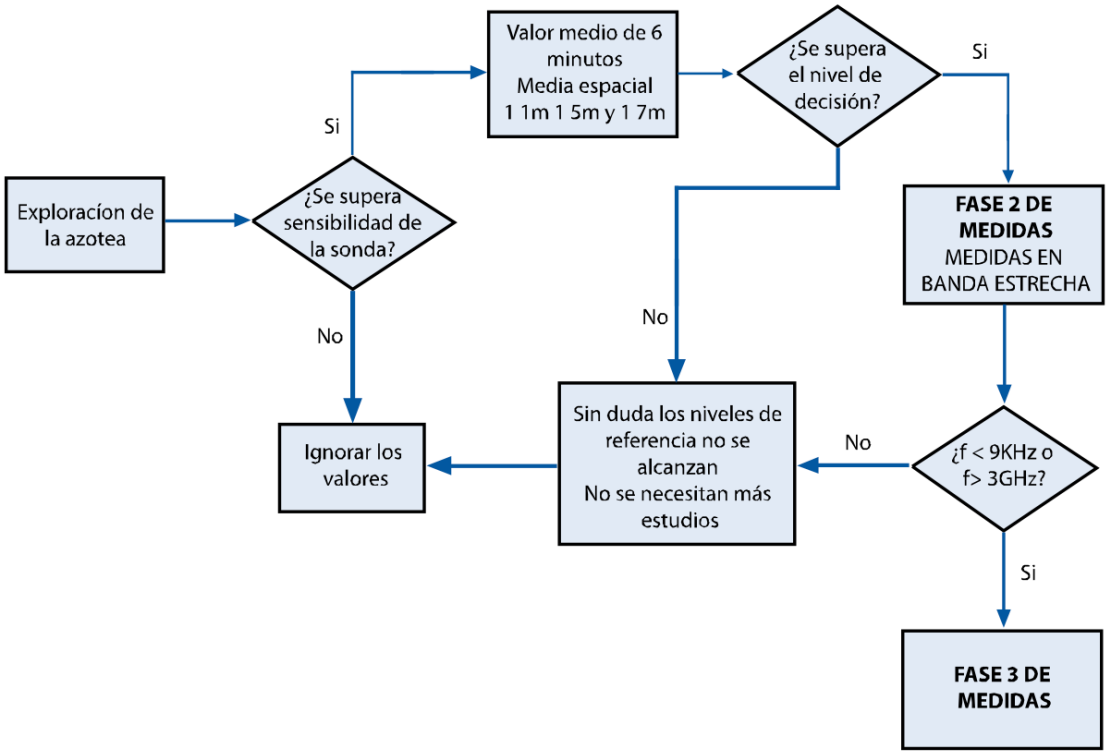
- Restricciones básicas: Los campos con estos niveles presentan efectos térmicos en las personas.
- Niveles de referencia: Niveles de intensidad de campos eléctricos, magnéticos y densidad de potencia para realizar las medidas experimentales y verificar que se cumplen las restricciones básicas.

La siguiente tabla presenta los niveles de referencia para la banda GSM900 y DCS1800 que han determinado diferentes organismos internacionales:

| Organismo | Grupo de exposición | Densidad de potencia equivalente [W/m^2] | |
|---|---|---|---|
| | | 900Mhz | 1800Mhz |
| ICNIRP | Ocupacional | 22,5 | 45 |
| ICNIRP | General | 4,5 | 9 |
| ANSI/IEEE | Ocupacional | 30 | 60 |
| ANSI/IEEE | General | 4,5 | 9 |
| FCC | Ocupacional | 22,5 | 45 |
| FCC | General | 4,5 | 9 |
| ARPANSA | Ocupacional | 30 | 50 |
| ARPANSA | General | 6 | 10 |
| Ministerio Salud Canadá | Ocupacional | 30 | 50 |
| Ministerio Salud Canadá | General | 6 | 10 |

Se puede observar que hay un factor 5 ó 6 entre el nivel de referencia ocupacional y el nivel de referencia general y la diferencia entre organismos reguladores, ya que los niveles de referencia tienen mayor o menor restricción. Para el caso de España se toman como niveles de referencia los del ICNIRP (Comisión internacional para la Protección contra las Radiaciones No Ionizantes).

La Orden CTE/23/2002 incluye un apartado en el que explica el procedimiento para la realización de las medidas de los niveles de emisión, que consta de diferentes fases resumidas en el siguiente diagrama:




**182. FASES PARAR LA MEDICIÓN DE UNA INSTALACIÓN**

Según establece la normativa, los estudios, certificaciones e informes relativos a estaciones radioeléctricas, deben ser visados en el Colegio profesional al que pertenezca el técnico competente que firme los trabajos. Para facilitar la gestión de visado, el Colegio Oficial de Ingenieros de Telecomunicación ha desarrollado la plataforma de visado telemático VisaTel© que facilita el visado y la tramitación de estas certificaciones.

La Ley 32/2003 General de Telecomunicaciones incorpora las normas de la Unión Europea, especificando que, como requisito esencial para la prestación de servicios radioeléctricos, se respeten los límites de potencia de emisión. El Artículo 53 habla de las infracciones muy graves, como por ejemplo: "Efectuar emisiones radioeléctricas que incumplan gravemente los límites de exposición establecidos en la normativa de desarrollo del artículo 44 de esta ley e incumplir gravemente las demás medidas de seguridad establecidas en dicha normativa, incluidas las obligaciones de señalización o vallado de las instalaciones radioeléctricas". El incumplimiento de los niveles establecidos puede dar lugar incluso a una inhabilitación de hasta cinco años del operador responsable.

Tras toda esta normativa, se elaboró un "Código de buenas prácticas para la instalación de infraestructuras de telefonía móvil" para agilizar todos los trámites. Un proyecto de despliegue de una instalación de telefonía móvil se resume en las siguientes fases administrativas:

- Paso 1. Aprobación del proyecto técnico de telecomunicaciones, conjuntamente con el estudio de niveles de exposición radioeléctrica y proyecto de instalación de señalización. Administración: Estado. Plazo para resolverse: 1 mes.

- Paso 1(bis). Otorgamiento de una licencia urbanística única que incluya la licencia de obras, instalación y actividad. Administración: Ayuntamiento. Plazo para resolverse: 3 meses.
- Paso 2. Una vez concedida la licencia urbanística y se han realizado las obras oportunas, deberá obtenerse una inspección favorable conforme a proyecto técnico. Administración: Estado. Plazo para resolver: 3 meses.
- Paso 3. Una vez que el operador aporte al Ayuntamiento el acta de inspección favorable, debe obtenerse la licencia de funcionamiento. Administración: Ayuntamiento. Plazo para resolver: 15 días.

Duración total: 6,5 meses

Tras este proceso dispondríamos de los medios legales para poder emitir con nuestra estación base y dar servicio a la zona que se pretendía.

Una vez vista la legislación referente a emisiones radioeléctricas, otra ley regula las licencias para poder emitir en diferentes bandas del espectro. La Orden Ministerial de 22 de septiembre de 1998 por la que se establecen el régimen aplicable a las licencias individuales para servicios y redes de telecomunicaciones y las condiciones que deben cumplirse por sus titulares.

En nuestro caso necesitaríamos una licencia de tipo B2:

*"2.2 Licencias de tipo B: Las licencias de tipo B habilitarán para la prestación del servicio telefónico disponible al público, mediante el establecimiento o la explotación, por su titular, de una red pública de telecomunicaciones*…

*…Licencias de tipo B2: Este tipo de licencias habilita para la prestación del servicio telefónico móvil disponible al público, mediante el establecimiento o explotación, por su titular, de una red pública telefónica móvil. Esta red podrá ser:*

*a) Red terrenal.*

*b) Red basada en satélites de órbita media o baja*."

*"SECCIÓN 3a LICENCIAS DE TIPO B*

*Artículo 25. Ámbito de las licencias de tipo B.*

*Las licencias de tipo B habilitarán para la prestación del servicio telefónico disponible al público, mediante el establecimiento o la explotación, por su titular, de una red pública de telecomunicaciones.*

*Las licencias de tipo B podrán ser de las siguientes categorías:*

*Licencias de tipo B1: Será necesaria una licencia de este tipo para la prestación del servicio telefónico fijo disponible al público, mediante el establecimiento o la explotación, por su titular, de una red pública telefónica fija. La explotación de la red incluye el derecho a prestar el servicio de líneas susceptibles de arrendamiento.*

*Licencias de tipo B2: Este tipo de licencias habilita para la prestación del servicio telefónico móvil disponible al público mediante el establecimiento o explotación, por su titular, de una red pública telefónica móvil. Esta red podrá ser:*

*a) Red terrenal o b) Red basada en satélites de órbita media o baja.*

*Las licencias de tipo B1 podrán ser de ámbito nacional o inferior. El ámbito territorial inferior al nacional deberá ser continuo, comprender municipios completos y alcanzar, como mínimo, una población de 50.000 habitantes.*

*Para el cálculo de esta cifra se utilizará la de la población de hecho, según los datos del último padrón municipal.*

*No obstante, cuando se haya obtenido la licencia por medio de licitación pública, el ámbito territorial será el establecido en el correspondiente pliego de bases.*

*Artículo 26. Derechos de los titulares de licencias de tipo B.*

*Los titulares de licencias de tipo B tendrán los siguientes derechos:*

*1. Obtener de la Comisión del Mercado de las Telecomunicaciones la asignación de los números que precisen para la prestación del servicio o para el establecimiento o explotación de la red para los que estén habilitados, de acuerdo con la normativa aplicable, especialmente, el Real Decreto por el que se aprueba el Reglamento sobre Interconexión y Numeración. Para la asignación de los números establecidos en el Plan Nacional de Numeración de los Servicios de Telecomunicaciones se seguirá el procedimiento previsto en el Real Decreto 225/1998, de 16 de febrero, por el que se aprueba el Reglamento de procedimiento de asignación y reserva de recursos públicos de numeración por la Comisión del Mercado de las Telecomunicaciones. En el ejercicio de este derecho, los titulares de licencias de tipo B1 que presten el servicio telefónico fijo disponible al público tendrán, además, los siguientes derechos:*

*Derecho a ser seleccionados mediante el procedimiento de llamada a llamada o mediante preselección.*

*Derecho a obtener códigos de selección de operador.*

*Los titulares de licencias de tipo B1 de ámbito nacional tendrán preferencia en la obtención de códigos de selección de cuatro cifras.*

*2. Interconectar la red que soporte la prestación del servicio telefónico disponible al público con las de los titulares de redes públicas, en los términos que se indican en este apartado. Cuando los titulares de redes públicas estén obligados a disponer de una oferta de interconexión de referencia, los titulares de licencias de tipo B tendrán derecho de interconexión en las centrales de conmutación locales y de nivel superior de conmutación, de acuerdo con lo dispuesto en el Reglamento de interconexión y numeración.*

*3. Ocupar, para el establecimiento o explotación de redes públicas, la propiedad pública o privada, en los términos establecidos en el capítulo II del título III de la Ley General de Telecomunicaciones y en el Reglamento de Obligaciones de Servicio Público.*

*A estos efectos, los solicitantes de licencias individuales que deseen que se les reconozcan, genéricamente, derechos de los regulados en el título III del Reglamento de Obligaciones de Servicio Público deberán hacerlo constar expresamente al órgano encargado de otorgar la licencia, bien en la solicitud inicial o bien mediante petición independiente si se hubiese otorgado ya el título. En dicha solicitud deberán asumir, asimismo, el compromiso de aceptar las obligaciones de servicio público que les sean impuestas.*

*En los supuestos a los que se refiere el párrafo anterior, en la resolución que otorgue la licencia individual para el establecimiento o explotación de una red pública de telecomunicaciones o en su modificación posterior, se recogerá el reconocimiento genérico de la posibilidad de ejercer derechos de ocupación de la propiedad pública o privada No obstante, lo dispuesto en este apartado, no tendrán*

*derecho a la ocupación del dominio público y de la propiedad privada los titulares de licencias de tipo B2 que presten el servicio telefónico disponible al público, mediante redes basadas en satélites de órbita media y baja.*

*4. Instalar terminales de uso público, situados en el dominio público, que permitan su uso común.*

*Artículo 27. Condiciones generales para titulares de licencias de tipo B.*

*1. Los titulares de licencias de tipo B deberán asumir el cumplimiento, además de las condiciones específicas que se les impongan en la correspondiente resolución de otorgamiento de la licencia y de las generales a que se refiere el artículo 5, de las siguientes:*

*1.1 Facilitar la interconexión y el acceso a sus redes, en los términos de lo establecido en la Ley General de Telecomunicaciones y en el Reglamento sobre interconexión y numeración.*

*1.2 Facilitar a la Comisión del Mercado de las Telecomunicaciones, de forma impresa y en soporte informático, los datos correspondientes a sus abonados para la confección de una guía unificada para cada ámbito territorial, en los términos de lo previsto en el artículo 37.1.b) de la Ley General de Telecomunicaciones y 14 del Reglamento de Obligaciones de Servicio Público y respetando, en todo caso, los derechos de los usuarios, especialmente, los contemplados en el artículo 54 de la misma Ley.*

*1.3 Garantizar, cuando sea preciso, la interconexión de las redes y la interoperabilidad de los servicios.*

*1.4 Si prestan el servicio telefónico disponible al público deberán establecer los procedimientos necesarios, de acuerdo con lo establecido en el Real Decreto de interconexión y numeración, para garantizar el derecho de los abonados a la conservación de los números.*

*1.5 Cuando así sea preciso por razones de interés general o de protección del medio ambiente, compartir sus infraestructuras con otros operadores, de conformidad con lo establecido en el artículo 47 de la Ley General de Telecomunicaciones.*

*1.6 Cumplir los compromisos de cobertura y extensión del servicio asumidos en su propuesta técnica y económica. No obstante, la Comisión del Mercado de las Telecomunicaciones, atendiendo a la consecución de un equilibrio entre los derechos y obligaciones del operador, podrá imponer un mínimo de cobertura y extensión del servicio o modificar los plazos del calendario propuesto.*

*1.7 Si prestan el servicio de líneas susceptibles de arrendamiento tendrán, además, las siguientes obligaciones:*

*Poner a disposición del público una oferta de líneas susceptibles de arrendamiento y presentársela, un mes antes de que surta efectos, a la Secretaría General de Comunicaciones y a la Comisión del Mercado de las Telecomunicaciones. En dicha oferta deberá incluirse la información relativa a las características técnicas, precios, condiciones generales de suministro y condiciones para la conexión de equipos terminales.*

*Formalizar un contrato con los usuarios, para el suministro del servicio.*

*Sólo podrán restringir el acceso a las líneas susceptibles de arrendamiento y su utilización cuando así lo exija el mantenimiento y la protección de los requisitos esenciales, tal y como se definen en el anexo de la Ley General de Telecomunicaciones.*

*No obstante, las condiciones señaladas en los apartados 1.2 y 1.5 no serán exigibles a los titulares de licencias de tipo B2 que presten el servicio telefónico móvil disponible al público mediante redes basadas en satélites de órbita media o baja.*

*2. Los titulares de licencias de tipo B1 deberán cumplir, también, las siguientes condiciones:*

*2.1 Facilitar a sus abonados la guía telefónica elaborada por ellos mismos o la que les suministre el operador obligado a ello, de acuerdo con el Reglamento de Obligaciones de Servicio Público.*

*2.2 En caso de que presten el servicio telefónico fijo disponible al público de ámbito nacional deberán establecer un punto de interconexión por provincia en el plazo de un año desde el comienzo de la prestación del servicio. Cuando la licencia de tipo B1 sea de ámbito inferior al nacional, sus titulares deberán establecer, desde el mismo momento del inicio de la prestación del servicio, al menos, un punto de interconexión en cada una de las provincias en las que vayan a prestar el servicio.*

*2.3 La red de ámbito territorial nacional que exploten deberá estar constituida de tal forma que, en el plazo de dos años, contado desde la fecha de otorgamiento de la licencia, al menos el 40 por 100 de sus medios de transmisión, calculado mediante la suma de los productos resultantes de multiplicar el número de kilómetros de cada circuito por el de kilobits/segundo de su capacidad, sea propio o haya sido arrendado mediante contratos con una vigencia mínima de cinco años. Este porcentaje deberá alcanzar el 60 por 100 a partir del tercer año, contado desde la fecha del otorgamiento de la licencia. A los efectos del cálculo del citado porcentaje, el alquiler de fibra óptica sin incluir equipos de conmutación o de terminación de fibra se considerará como red propia.*

*2.4 Para los titulares de licencias de tipo B1 de ámbito territorial inferior al nacional, la Comisión del Mercado de las Telecomunicaciones, en función de las condiciones concretas de cobertura y extensión de las redes y de los servicios que se les impongan y con arreglo a los principios de objetividad y proporcionalidad, establecerá las exigencias específicas a que se refieren los apartados 2.3 y 2.4 de este artículo que le serán de aplicación.*

*3. Los operadores de licencias de tipo B1, cuando tengan la consideración de dominantes con arreglo a lo establecido en el artículo 23 de la Ley General de Telecomunicaciones, deberán cumplir lo dispuesto en el apartado I del anexo I de esta Orden."*

# BIBLIOGRAFÍA


[1] CNMC, "Informe anual," 2014.

[2] (2015) Wikipedia. [Online]. https://en.wikipedia.org/wiki/GSM#/media/File:GSMLogo.svg

[3] Mónica Gorricho Moreno and Juan Luis Gorricho Moreno, *Comunicaciones Móviles*, 1st ed. Barcelona, España: Ediciones UPC, 2002.

[4] Oriol Sallent Roig, José Luis Valenzuela González, and Ramón Agustí Comes, *Principios de comunicaciones móviles*, 1st ed. Barcelona, España: Editorial UPC, 2003.

[5] La Vanguardia, "Primera demostración pública del sistema de telefonía celular PAN-Europea GSM," *La Vanguardia*, p. 55, July 1991.

[6] La Vanguardia, "De la telefonía móvil a la telefonía portátil," *La Vanguardia*, Oct. 1990.

[8] Lorena González. (2015, May) Rankia. [Online]. http://www.rankia.com/blog/tarifas-moviles/1988642-diferencias-sim-microsim-nanosim

[7] Tsaitgaist. (2015) Wikipedia. [Online]. https://commons.wikimedia.org/wiki/File:Gsm_structures.svg

[9] Rauf Akram. (2014, Feb.) Rauf Akram blog. [Online]. https://raufakram.wordpress.com/2014/02/11/uicc-multi-sim-the-jargon/

[10] Daniel Haro. Flexi EDGE BTS & MSR HW. O&M.

[11] Cosenic. Attacking the GSM baseband and base station.

[12] Liz Delacour. (2009, Mar.) Red celular. [Online]. http://redcelular12b.blogspot.com.es

[13] Range Networks. (2014) OpenBTS Logo. [Online]. http://openbts.org/documentation.php

[14] Range Networks. OpenBTS. [Online]. http://openbts.org/about/

[15] Range Networks. (2015) OpenCell Series. [Online]. http://www.rangenetworks.com/products/open-cell-series

[16] OpCom. Open Communications. Voix sur IP. [Online]. http://www.opcom.fr/?cPath=1

[18] Agilent Technologies. (2009) Spectrum Analyzer Mode. Measurement Guide.

[17] Netelip. (2015) ¿Por qué elegir la Centralita Virtual de netelip? [Online]. http://netelip.com/es/centralita-virtual-vpbx-centralita-voip

[19] André L. G. Reis, André F. B. Selva, Karlo G. Lenzi, Sílvio E. Barbin, and Luís G. P. Meloni, "Software Defined Radio on Digital Communications: a New Teaching Tool," in *Wireless and Microwave Technology Conference (WAMICON)*, Cocoa Beach, 2012, pp. 1-8.

[20] N. Prasannan et al., "OpenBTS based microtelecom model: A socio-economic boon to rural communities," in *Automation, Computing, Communication, Control and Compressed Sensing*

*(iMac4s)*, Kottayam, 2013, pp. 856 - 861.

[21] TS 51.021, "Base Station System (BSS) equipment specification ," 3GPP,.

[22] TS 45.005, "Radio transmission and reception ," 3GPP,.

[23] TS 45.004, "Technical Specification Group GSM/EDGE Radio Access Network; Modulation ," 3GPPP,.

[24] TS 45.001, "Physical layer on the radio path; General description ," 3GPP,.

[25] Jorge Navarro Ortiz, "Seguridad en Redes Inalámbricas," Universidad de Granada, 2014.

[26] José C. Segura, "Comunicaciones II," Universidad de Granada,.

[27] José Maria Hernando Rábanos, "Comunicaciones Móviles,".

# ÍNDICE

**ACP**, 69

**Ancho de banda ocupado**, 70, 71, 74

Asterisk, 50, 52, 53, 54, 57, 59, 60, 92, 93, 94, 95, 98, 99, 100, 101, 104, 105, 106, 109, 110, 112, 119

**BCCH**, 37, 39, 42, 84, 88

BSC, 30, 44, 50

BTS, 30, 32, 39, 43, 44, 45, 50, 54, 55, 56, 63, 76, 81, 82, 83, 84, 86, 88, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117

DCS1800, 37, 51, 52, 73, 74, 79, 80

ecualización del canal, 39, 40, 103

**FACCH**, 37, 40, 53

**FCCH**, 39, 41, 53

FDD, 37

FDMA, 37

GMSK, 33, 34, 35, 52, 71, 76, 77, 79

GPRS, 22, 23, 27, 47, 49, 50, 51, 53, 97, 98, 119

GSM, 19, 22, 23, 24, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 43, 45, 49, 50, 52, 53, 54, 55, 56, 57, 61, 63, 65, 66, 67, 68, 69, 70, 73, 75, 77, 80, 82, 83, 84, 88, 90, 95, 96, 97, 112, 113, 114, 115, 116, 117, 119, 120, 129, 134, 135, 137, 138

GSM900, 38, 51, 66, 74, 79, 80

GSMTAP, 67, 83, 84

HLR, 29, 30, 43, 50, 54

IMSI, 23, 29, 30, 31, 42, 51, 54, 55, 63, 86, 90, 93, 94, 97, 98, 99, 100, 101, 102, 134, 135, 136, 137

interferencia intersimbólica, 35, 76

Ley 32/2003, General de Telecomunicacione, 138

**Máscara del espectro de emisión**, 72, 74, 75

MSC, 30, 32, 42, 43, 44, 50, 57, 58

NodeManager, 52, 54, 60

OpenBTS, 23, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 60, 65, 67, 68, 69, 73, 88, 89, 112, 113, 114, 116, 118, 119, 120, 122, 125, 126, 127, 128, 129, 134

OpenBTSCLI, 52, 55, 128

OsmocomBB, 23, 50, 61, 62, 63, 64, 65, 67, 129, 131, 132, 134

**PAGCH**, 37, 39, 44

PAGING, 44

**Potencia del canal**, 69, 73

**RACH**, 37, 39, 40, 42, 43, 84

ráfagas, 27, 35, 40, 53

red celular, 22, 23, 24

**SACCH**, 37, 40, 53, 88, 92

**SCH**, 37, 39, 41, 42, 53

**SDCCH**, 40, 53, 90

SDR, 23, 50, 51, 52, 67, 68, 69, 73, 79, 116, 117, 122, 126, 128, 134

servicio troncal de llamadas VoIP, 58

SIM, 23, 28, 29, 50, 54, 62, 63, 93, 116, 134, 135, 137

símbolo, 52, 76, 79

SIPAuthServe, 52, 53, 54, 99

SMS, 23, 27, 30, 32, 41, 45, 50, 53, 55, 56, 62, 63, 64, 65, 112, 113, 114, 115, 117, 118, 134, 135, 136

**TCH**, 37, 40, 53, 64, 88

TDMA, 37, 38

*timeslot*, 89

TMSI, 42

Transceiver, 52, 129

VLR, 29, 30, 42, 43, 44, 50, 54