

4 Red GSM

4.1 Introducción al estándar GSM

Formalmente conocida como "*Group Special Mobile*" (GSM, Grupo Especial Móvil) aunque también llamada *Global System for Mobile communications* (Sistema Global para las Comunicaciones Móviles), por el influjo del mundo anglosajón, es un estándar mundial para teléfonos móviles digitales creado por la CEPT y posteriormente desarrollado por el ETSI como un estándar para los teléfonos móviles europeos, con la intención de desarrollar una normativa que fuera adoptada mundialmente. El estándar es abierto, no propietario y evolutivo (aún en desarrollo) y es el estándar predominante en Europa, así como el mayoritario en el resto del mundo (alrededor del 80% de los usuarios de teléfonos móviles del mundo en 2004 usaban GSM). GSM difiere de sus antecesores principalmente en que tanto los canales de voz como las señales son digitales. Para lograr así un moderado nivel de seguridad.

GSM tiene cuatro versiones principales basadas en las bandas: GSM-850, GSM-900, GSM-1800 y GSM-1900. GSM-900 (900 MHz) y GSM-1800 (1,8 GHz) son utilizadas en la mayor parte del mundo, salvo en Estados Unidos, Canadá y el resto de América Latina, lugares en los que se utilizan las bandas de GSM-850 y GSM-1900 (1,9 GHz), ya que en EE.UU. las bandas de 900 y 1800 MHz están ya ocupadas para uso militar. Inicialmente, GSM utilizó la frecuencia de 900 MHz, pero tras su rápida expansión, pronto se saturó el espacio radioeléctrico entorno a esa frecuencia por lo que las redes de telecomunicación pública empezaron a utilizar las frecuencias de 1800 y 1900 MHz, con lo cual es habitual que los equipos móviles de hoy en día sean tribanda.

Desde un principio, los creadores de GSM intentaron lograr la compatibilidad con la RDSI en términos de servicios ofrecidos y señalización de control utilizada, sin embargo, las limitaciones del radioenlace en términos de ancho de banda y costes no permitieron que los estandarizados 64 Kbps de tasa de transmisión de un canal B sobre RDSI se alcanzaran en la práctica.

Utilizando las definiciones de la ITU-T, los servicios de telecomunicaciones se pueden dividir en portadores, teleservicios y servicios suplementarios, siendo sin duda el servicio más destacado el de la telefonía. No obstante, una gran variedad de servicios son ofrecidos por la red. Sus usuarios pueden enviar y recibir datos a una velocidad de hasta 9,600 bps a usuarios que utilicen la red telefónica conmutada, RDSI y redes públicas de conmutación de paquetes y circuitos utilizando una amplia gama de protocolos como X.25 y X.32, con la ventaja adicional de no necesitar módem al ser digital para dialogar con estas redes, excepto para comunicaciones vocales con la PSTN. Otros servicios de datos incluyen fax grupo 3 según se describe en la recomendación T.30 de la ITU-T.

El único servicio ofrecido por GSM y que no se encuentra en los sistemas analógicos más antiguos es el que realmente nos interesa para este proyecto, el servicio de mensajes cortos o SMS (Short Message Service). SMS es un servicio bidireccional para mensajes alfanuméricos cortos (hasta 160 bytes).

4.1.1 Arquitectura de la red GSM

En la Figura 4.1 se muestra de manera resumida la arquitectura de la red GMS. Esta arquitectura es más compleja y dispone de más elementos que los presentados en esta figura. El objetivo de esta introducción es describir el servicio SMS a nivel de aplicación, sin entrar en demasiados detalles de la red subyacente.

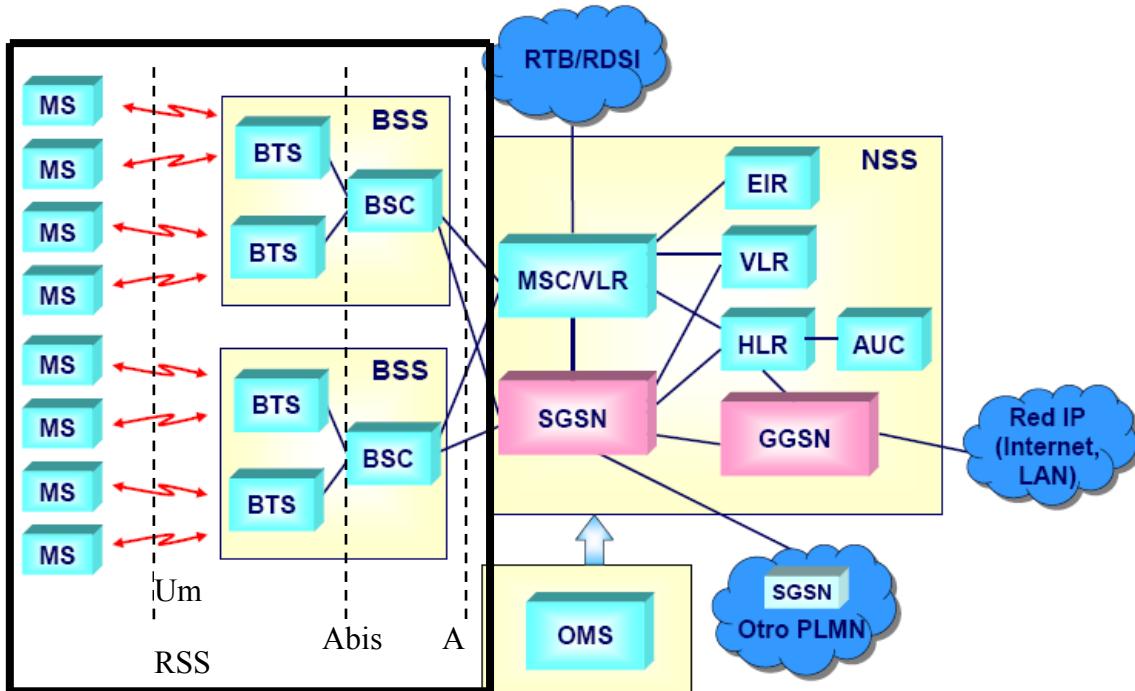


Figura 4.1 Arquitectura de la red GSM

A continuación se detallarán resumidamente los principales bloques del diagrama mostrado en la Figura 4.1:

1. **Subsistema Radio (RSS, Radio SubSystem).** Cubre la comunicación entre las estaciones móviles (MS) y las estaciones base (BTS). El interfaz radio entre ellas se denomina Um.
2. **El subsistema de estaciones base (BSS),** incluido dentro de la parte Radio, está constituido por los siguientes elementos:
 - a. **BTS (Base Transceiver Station):** emisor, receptor y antena. Procesa los canales radio (Interfaz Um).
 - b. **BSC (Base Station Controller):** Handover, control de las BTS, mapeo de canales radio sobre los canales terrestres. Por un lado se comunica con las BTS a través de un interfaz con canales de 16kbits/s (Abis) y por otro lado se comunica con los MSC a través del interfaz A, con canales de 64kbits/s.

Este subsistema hace de interfaz entre la parte radio y la parte de red.

3. **Subsistema de red y conmutación (NSS, Network and Switching Subsystem).** Conmutación, gestión de la movilidad, interconexión con otras redes y control

del sistema. Esta es la parte más compleja, siendo sus elementos fundamentales los siguientes:

- a. **MSC (Mobile Services Switching Center)**, centro de conmutación entre otras muchas funciones.
- b. **GMSC (Gateway Mobile Services Switching Center)**. Conexión con otras redes.
- c. **Bases de datos**:
 - i. **HLR (Home Location Register)**.
 - ii. **VLR (Visitor Location Register)**.
 - iii. **EIR (Equipment Identity Register)**.

4.1.2 La trama GSM

Para la transmisión de “bits” entre la estación base y una estación móvil se utilizan canales físicos, caracterizados por un número de slot y una portadora. Dentro de cada portadora, capaz de transportar una multitrama se multiplexan en el tiempo 8 ranuras, formando una trama TDMA. En el gráfico de la Figura 4.2 se ha detallado una de estas tramas de tráfico aunque las hay de otros tipos. Cabe indicar que dentro de los 26 slots de la multitrama, el 12 esta reservado para señalización y el 25 no se utiliza, siendo el resto canales de datos.

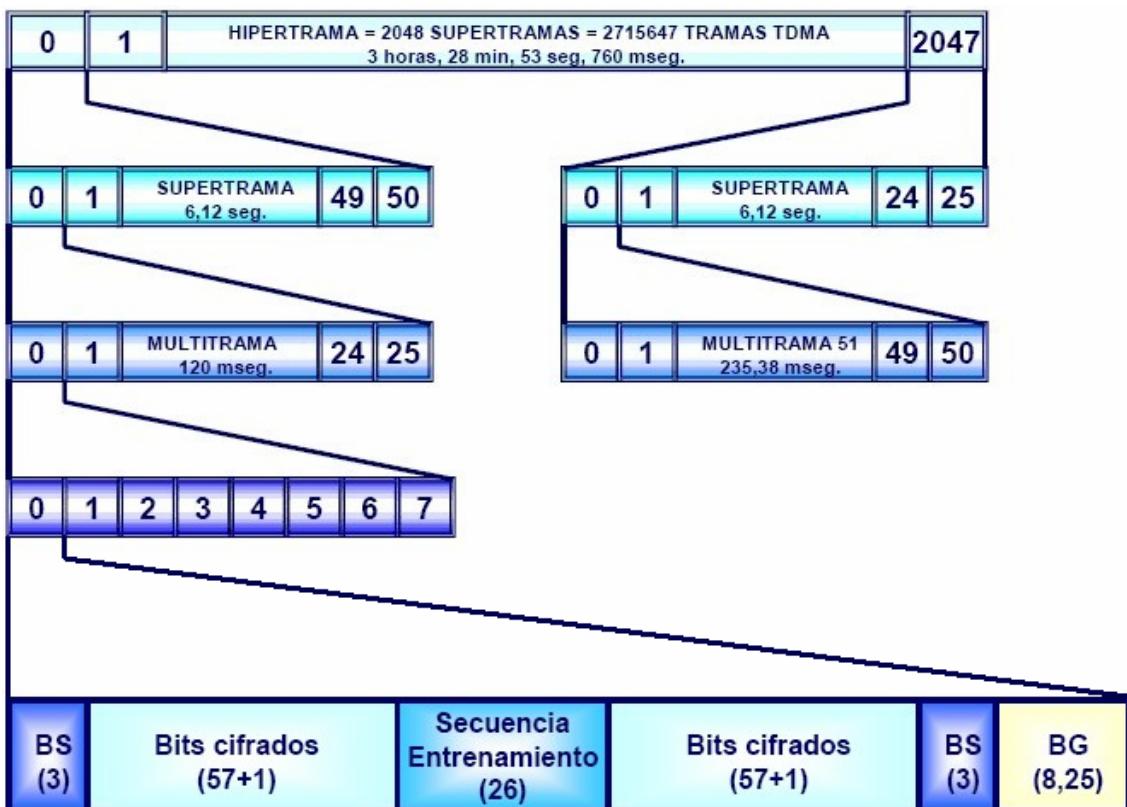


Figura 4.2 Diagrama de entrampado GSM

A un nivel superior, los canales físicos se dividen en:

- Canales de tráfico: Llevan la voz y/o los datos
- Canales de Control: señalización y señales de control.

Los canales de tráfico pueden ser de 2.4, 4.8 ó 9.6Kb/s. Para el servicio SMS se utilizan canales de control.

4.2 SMS

4.2.1 Servicio SMS

El servicio SMS, esquematizado en la Figura 4.3, permite transferir un mensaje de texto entre una estación móvil (MS) y otra entidad (SME) a través de un centro de servicio (SC). El servicio final ofrecido es una comunicación extremo-extremo entre la estación móvil (MS) y la entidad (SME). La entidad puede ser otra estación móvil o puede estar situado en una red fija. En el caso de envío de un mensaje entre dos móviles, ambas partes son estaciones móviles. Cuando se envía un mensaje para solicitar algún tipo de servicio de valor añadido, un extremo es una estación móvil y la otra es un servidor que atiende las peticiones, como puede ser uno de los exitosos sistemas de televoto actuales.

En la norma GSM sólo se especifica la parte de comunicaciones entre las estaciones móviles (MS) y el Centro de servicio. La comunicación entre el Centro de Servicio y las entidades fijas, queda fuera del ámbito de esta norma.

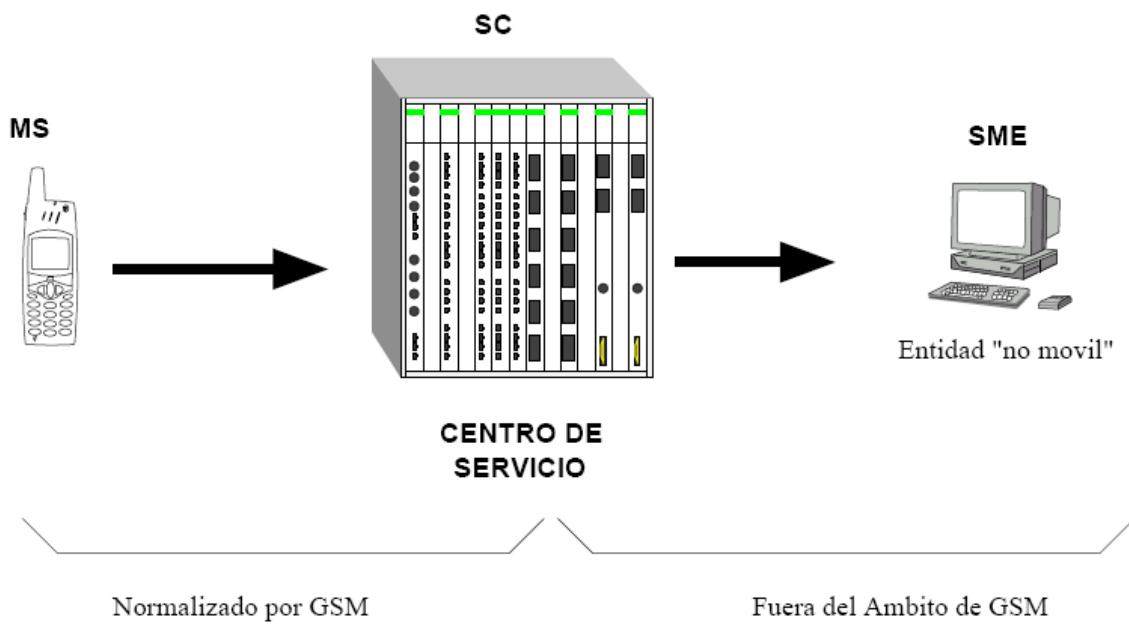


Figura 4.3 *Estructura del servicio SMS*

El servicio SMS se divide en dos servicios Básicos detallados en la Figura 4.4:

1. SM MT (Short Message Mobile Terminated Point-to-Point). Servicio de entrega de un mensaje desde el SC hasta una MS, obteniéndose un informe sobre lo ocurrido.
2. SM MO (Short Message Mobile Originated Point-to-Point). Servicio de envío de un mensaje desde una MS hasta un SC, obteniéndose un informe sobre lo ocurrido.

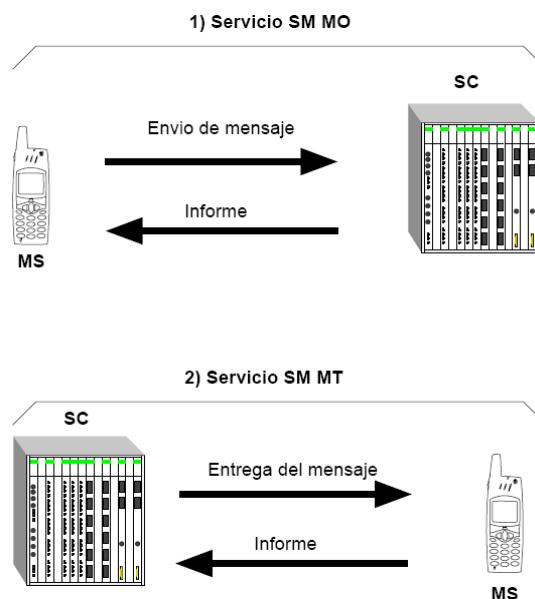


Figura 4.4 *Servicios básicos SM MO y SM MT*

4.2.2 Arquitectura

La estructura básica de la red para el servicio SMS consta de las siguientes entidades:

- MS: Estación móvil.
- MSC: Centro de conmutación.
- SMS-GMSC: MSC pasarela para el servicio de mensajes cortos (Servicio SM MT).
- SMS-IWMSC: MSC de interconexión entre PLMN y el SC (Servicio SM MO).
- SC: Centro de Servicio.
- HLR, VLR.

4.2.3 Modelo de capas

Para la descripción detallada de la arquitectura, se utiliza un modelo de capas (Figura 4.5), en el que cada capa o nivel proporciona un servicio a la capa superior, y este servicio se implementa mediante el protocolo correspondiente. La arquitectura se divide en 4 capas:

- **SM-AL (Short Message Application Layer): Nivel de aplicación.**

- **SM-TL (Short Message Transfer Layer): Nivel de transferencia.** Servicio de transferencia de un mensaje corto entre una **MS** y un **SC** (en ambos sentidos) y obtención de los correspondientes informes sobre el resultado de la transmisión. Este servicio hace abstracción de los detalles internos de la red, permitiendo que el nivel de aplicación pueda intercambiar mensajes.
- **SM-RL (Short Message Relay Layer): Nivel de repetición.** Proporciona un servicio al nivel de transferencia que le permite enviar TPDU (Transfer Protocol Data Units) a su entidad gemela.
- **SM-LL (Short Message Lower Layers): Niveles inferiores.**

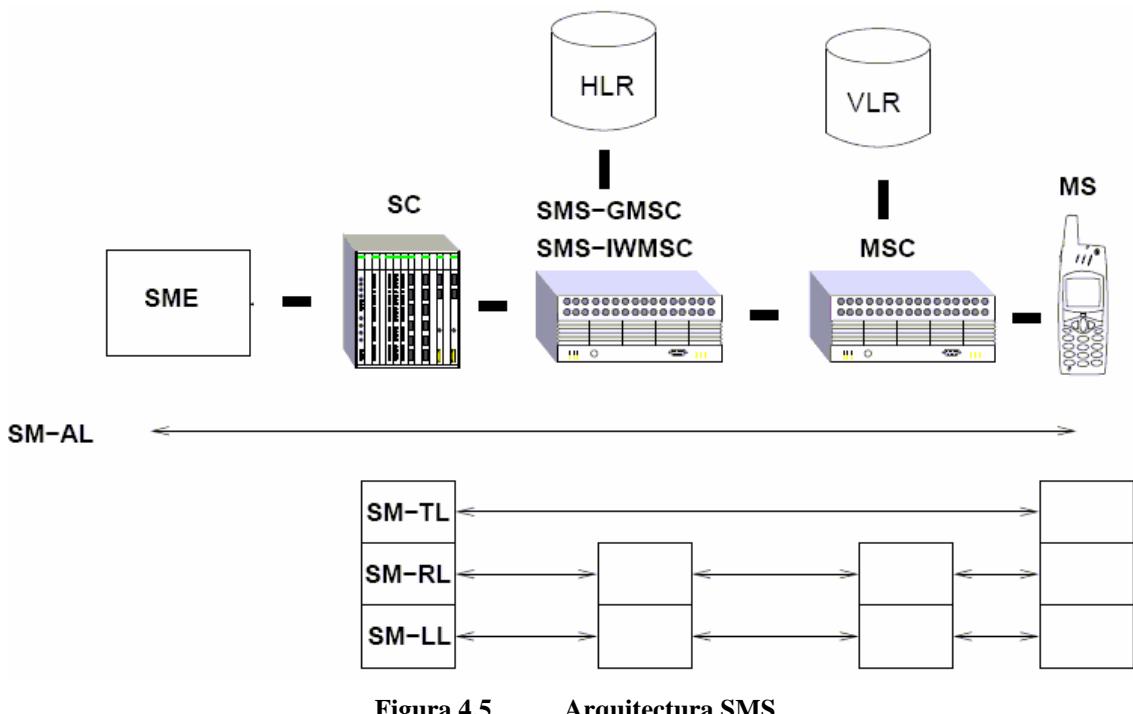


Figura 4.5 Arquitectura SMS

Cada capa proporciona los servicios a la capa superior utilizando un protocolo. Se definen los protocolos SM-TP y SM-RP, que se corresponden con las capas SM-RL y SM-TL. **El nivel de interés es el SM-TL**, que es el que se usará para enviar y recibir SMS.

El servicio proporcionado por la **capa SM-TL** permite al nivel de aplicación enviar mensajes a su entidad gemela, recibir mensajes de ella así como obtener informes sobre el estado de transmisiones anteriores. Para hacerlo se utilizan las siguientes PDUs:

- **SMS-DELIVER:** Transmitir un mensaje desde el SC al MS.
- **SMS-DELIVER-REPORT:** Error en la entrega (si lo ha habido).
- **SMS-SUBMIT:** Trasmitir un mensaje corto desde el MS al SC.
- **SMS-SUBMIT-REPORT:** Error en la transmisión (Si lo ha habido).
- **SMS-STATUS-REPORT:** Transmitir un informe de estado desde el SC al MS.
- **SMS-COMMAND:** Transmitir un comando desde el MS al SC.

4.2.3.1 SMS-SUBMIT

La estructura de la PDU **SMS-SUBMIT** se muestra en la Figura 4.6. Para el caso también interesante de una PDU **SMS-DELIVER**, la estructura es tremadamente similar y no se detallará. Los campos que la componen son los siguientes:

- **SCA:** Número de teléfono del Centro de Servicio (SC). La estructura detallada se muestra en la Figura 4.7. Consta de los siguientes campos:
 - **Longitud:** Número de dígitos del teléfono del SC.
 - **Tipo de número:** Indica si se trata de un número nacional o internacional:
 - **81h:** Nacional.
 - **91h:** Internacional.
 - **Dígitos BCD:** Número de teléfono del SC, en dígitos BCD.
- **PDU-TYPE:** Contiene información sobre el tipo de PDU:
 - **RP:** Existe camino de respuesta. RP=0 en tramas de tipo SMS-SUBMIT.
 - **UDHI:** Indica si el campo UD contiene sólo el mensaje corto (UDHI=0) o si existe una cabecera antes del mensaje corto (UDHI=1).
 - **SRR:** Informe de estado no solicitado (SRR=0) o sí solicitado (SRR=1).
 - **VPF:** Indica si el campo VP está o no presente.
 - **RD:** Rechazar o no duplicados.
 - **MTI:** Tipo de mensaje.
- **MR:** Parámetro para identificar el mensaje.
- **DA:** Dirección del SME destino (número de teléfono).
- **PID:** Identificación del protocolo de la capa superior.
- **DCS:** Identificación del tipo de codificación dentro de los datos de usuario.
- **VP:** Periodo de validez del mensaje.
- **UDL:** Longitud del campo UD.
- **UD:** Datos de usuario.

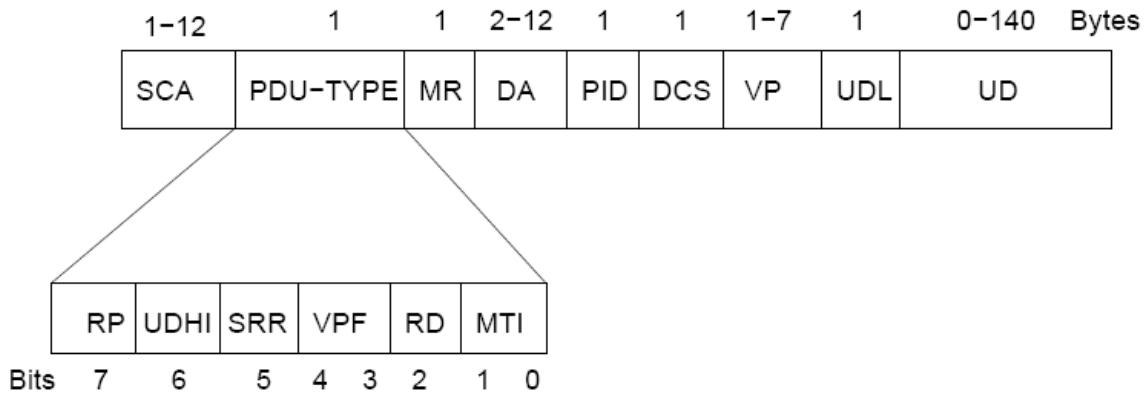


Figura 4.6 Estructura de la PDU SMS-SUBMIT

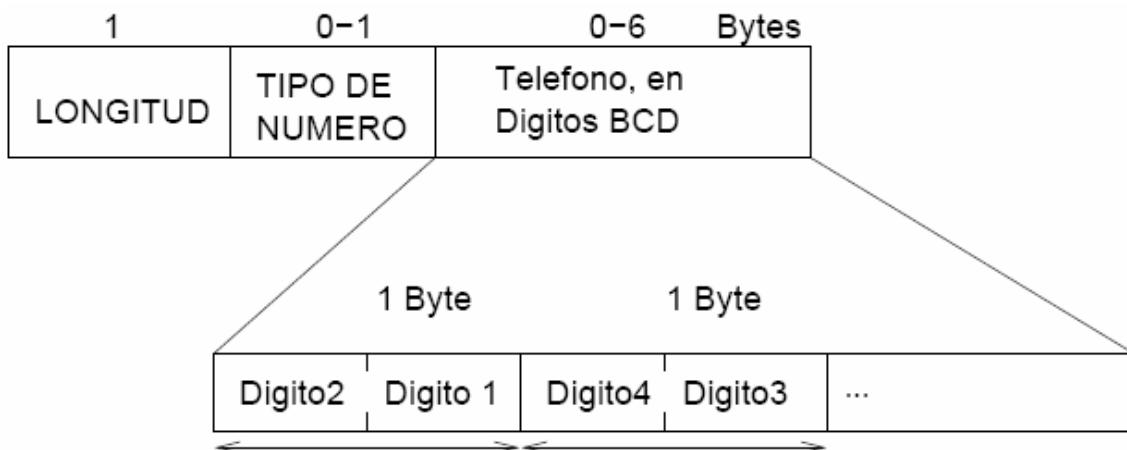


Figura 4.7 Detalle del campo SCA

Si quisiéramos enviar el mensaje corto “hola” al teléfono 630672901 utilizando el Centro de mensajes +341710760000.

- **SCA:** 0C91437101670000 (8 bytes)

Longitud	Tipo	Tlf en BCD
0C	91	43-71-01-67-00-00

- **PDU-TYPE:** 01h. Trama de tipo **SMS-SUBMIT**. Campo de usuario sin cabecera. Informe de estado no solicitado. Campo VP no presente.

RP	UDHI	SRR	VPF	RD	MTI
0	0	0	0 0	0	0 1

- **MR:** 00h. Número de referencia 0.
- **DA:** 0681366027091F (7 bytes). Teléfono destino.

Longitud	Tipo	Tlf en BCD
09	81	36-60-27-09-F1

- **PID:** 00h (mensaje corto).

- **DCS:** F6h (Codificación de 8 bits, en ASCII).
- **UDL:** 04. Longitud de los datos de usuario.
- **UD:** 686F6C61 (4 bytes). Datos de usuario.

h	o	1	a
68	6F	6C	61

La trama final montada es la mostrada en la Figura 4.8 que ocupa un total de 24 bytes para enviar sólo cuatro.

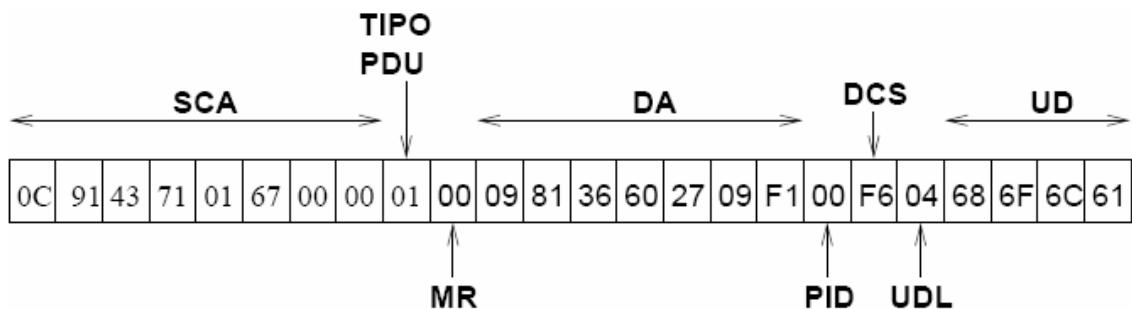


Figura 4.8 Ejemplo de PDU SMS

4.3 Los comandos AT

Los comandos AT (se denominan así por la abreviatura de *attention*) son instrucciones codificadas que conforman un lenguaje de comunicación entre el hombre y un terminal módem. En un principio, el juego de comandos AT fue desarrollado en 1977 por Dennis Hayes como un interfaz de comunicación con un módem para así poder configurarlo y proporcionarle instrucciones, tales como marcar un número de teléfono. Más adelante, con el avance del baudio, fueron las compañías Microcomm y US Robotics las que siguieron desarrollando y expandiendo el juego de comandos hasta universalizarlo.

Aunque la finalidad principal de los comandos AT es la comunicación con módems, la telefonía móvil GSM también ha adoptado como estándar este lenguaje para poder comunicarse con sus terminales. De esta forma, todos los teléfonos móviles GSM poseen un juego de comandos AT específico que sirve de interfaz para configurar y proporcionar instrucciones a los terminales. Este juego de instrucciones puede encontrarse en la documentación técnica de los terminales GSM y permite acciones tales como realizar llamadas de datos o de voz, leer y escribir en la agenda de contactos y enviar mensajes SMS, además de muchas otras opciones de configuración del terminal.

Los comandos AT con cadenas ASCII que comienzan por los caracteres AT y terminan con un *retorno de carro (LF)*. Cada vez que el módem recibe un comando, lo procesa y devuelve un resultado, que normalmente es una cadena ASCII salvo que hayamos indicado lo contrario. Al estar la comunicación en ASCII, pondremos utilizar

un terminal de comunicaciones desde un ordenador para acceder al módem, bien para configurarlo, bien para hacer pruebas o bien para establecer una comunicación con otro módem.

Los módems GSM no sólo se comportan de forma muy parecida a un módem normal, permitiendo el intercambio de datos con otro módem y utilizándose los comandos AT originales, sino que incluyen muchas más características. Son como pequeños teléfonos móviles, que incluyen su propia tarjeta SIM para poder funcionar y por tanto permiten gestionar la base de datos de teléfonos, la lista de los mensajes SMS recibidos, enviar mensajes SMS, configurar diversos parámetros...

Para tener acceso a todos esos servicios, y dado que los comandos AT estaban muy extendidos y muy estandarizados, se ha realizado una ampliación, añadiéndose nuevos comandos. Estos nuevos comandos comienzan por los caracteres AT+, y se denominan comandos AT+. Mostramos a continuación la estructura general de estos comandos en un sencillo ejemplo:

- Petición:

AT+CMGI<CR> //Donde <CR> simboliza el retorno de carro.

- Respuesta correcta:

<CR><LF>Siemens mobile phones<CR><LF>
<CR><LF>OK<CR><LF> //Donde <LF> simboliza nueva línea.

- Respuesta errónea:

<CR><LF>ERROR<CR><LF>

Indiquemos, llegados a este punto, que el código no es sensible al uso de mayúsculas o minúsculas y que la tecla “intro” de un PC tipo qwerty envía al terminal los caracteres retorno de carro y nueva línea.

4.3.1 Listado de comandos AT y AT+ más frecuentes

1. Comandos generales

- AT+CGMI: Identificación del fabricante.
- AT+CGSN: Obtener número de serie.
- AT+CIMI: Obtener el IMSI.
- AT+CPAS: Leer estado del módem.

2. Comandos del servicio de red

- AT+CSQ: Obtener calidad de la señal.
- AT+COPS: Selección de un operador.
- AT+CREG: Registrarse en una red.
- AT+WOPN: Leer nombre del operador.

3. Comandos de seguridad:

- AT+CPIN: Introducir el PIN.
- AT+CPINC: Obtener el número de reintentos que quedan.
- AT+CPWD: Cambiar password.

4. Comandos para la agenda de teléfonos

- a. **AT+CPBR**: Leer todas las entradas.
- b. **AT+CPBF**: Encontrar una entrada.
- c. **AT+CPBW**: Almacenar una entrada.
- d. **AT+CPBS**: Buscar una entrada.

5. Comandos para SMS

- a. **AT+CPMS**: Seleccionar lugar de almacenamiento de los SMS.
- b. **AT+CMGF**: Seleccionar formato de los mensajes SMS.
 - i. Modo texto
 - ii. Modo PDU
- c. **AT+CMGR**: Leer un mensaje SMS almacenado.
- d. **AT+CMGL**: Listar los mensajes almacenados.
- e. **AT+CMGS**: Enviar mensaje SMS.
- f. **AT+CMGW**: Almacenar mensaje en memoria.
- g. **AT+CMSS**: Enviar mensaje almacenado.
- h. **AT+CSCA**: Establecer el Centro de mensajes a usar.
- i. **AT+WMSC**: Modificar el estado de un mensaje.

4.3.2 Algunos ejemplos

A continuación se muestran algunos ejemplos de utilización de los comandos AT+. Para probarlos se ha utilizado un ordenador PC, un módem GSM conectado al puerto serie y un terminal de comunicaciones. En nuestro caso, se ha empleado la aplicación “Hyperterminal” de Microsoft que se incluye como utilidad en cualquier sistema operativo Windows.

Listado de mensajes

Los mensajes cortos se dividen en 5 categorías, cada una identificada por una cadena. Para listar los mensajes se utiliza el comando **AT+CMGL=<categoría>**, donde *<categoría>* es una cadena de texto que puede valer lo siguiente:

- “**REC UNREAD**”: Mensajes recibidos pero no leídos.
- “**REC READ**”: Mensajes recibidos y leídos.
- “**STO UNSEND**”: Mensajes escritos y almacenados pero no enviados.
- “**STO SENT**”: Mensajes enviados.
- “**ALL**”: Todos los mensajes.

A continuación se leen todos los mensajes:

AT+CMGL="ALL"

```
+CMGL: 1, "REC READ", "609", "05/02/27,18:16:51+40"
Como cliente MoviStar Plus Elección, esta de enhorabuena.
Porque desde el 18 de febrero esta ahorrando un 49 % en sus
llamadas de móvil a fijo en horario normal
+CMGL: 2, "REC READ", "1122", "05/02/28,20:41:25+40"
```

-Bienvenido a Omitel Movistar! Para acceder a su buzón de voz marque 123, servicio de Atención al Cliente marque 609 (llamadas no gratuitas desde el extranjero)
 +CMGL: 3,"REC READ","+34609100609","05/05/06,10:00:16+04"
 Telefónica MoviStar le desea una feliz estancia. Para llamar al CRC MoviStar marque +34 609 100 609. Para llamar a su Buzón de Voz marque +34 609 123 123
 OK

Lectura de un mensaje

Se utiliza el comando **AT+CMGR=<número>**, donde *<número>* es el número del mensaje a leer.

AT+CMGR=1

+CMGR: "REC READ", "609", "05/02/27,18:16:51+40"
 Como cliente MoviStar Plus Elección, esta de enhorabuena.
 Porque desde el 18 de febrero esta ahorrando un 49 % en sus llamadas de móvil a fijo en horario normal
 OK

Si se especifica un número de mensaje que no existe se devuelve un mensaje de error:

AT+CMGR=4

ERROR

Borrar un mensaje

Se utiliza el comando **AT+CMGD=<numero>**, donde *<número>* hace referencia al número de mensaje a borrar.

AT+CMGD=3

OK

Mensaje Borrado. Si ahora se intenta leer:

AT+CMGR=3

ERROR

Envío de un SMS en modo texto

Para enviar un mensaje SMS se puede realizar de dos maneras diferentes. Se puede utilizar el **modo texto**, en que sólo hay que indicar el número de teléfono y el contenido del mensaje. Es el módem el que se encarga de generar la trama SMS-SUBMIT correspondiente y enviarla. Este es el modo que normalmente se emplea si sólo queremos transmitir un mensaje pues simplifica mucho el proceso.

Es posible tener acceso directamente al protocolo **SM-TP**, enviando directamente una trama de tipo SMS-SUBMIT. En este caso se habla de **modo PDU**.

Será el nivel de aplicación el que tendrá que generar correctamente la trama SMS-SUBMIT y el módem simplemente la transmitirá.

La configuración del módem para funcionar en uno u otro modo se realiza mediante el comando **AT+CMGF=<modo>**, donde *<modo>* puede tener los siguientes valores:

- *<modo>*=1: **Modo texto**
- *<modo>*=0: **Modo PDU** (Modo por defecto)

Para enviar un mensaje en **modo texto**, se utiliza el comando **AT+CMGS**. Primero se especifica el número de teléfono, seguido de un carácter retorno carro **<CR>**. El módem responde enviando el carácter “>” que indica que se puede escribir el mensaje que se quiere enviar. Para delimitar el mensaje hay que enviar el carácter **<control-z>** (Es el carácter ASCII 26).

Si el mensaje se ha enviado correctamente, devuelve la cadena “**+CMGS:<nr>**” seguida del **OK**. El campo *<nr>* es el número de referencia del mensaje, que se va incrementando, tomando los valores comprendidos entre 0 y 255, cada vez que se envía un SMS.

```
AT+CMGS="630672901"<CR>
>Mensaje de prueba <control-z>
+CMGS: 2
OK
```

Puesto que hemos enviado un auto-mensaje (un mensaje SMS con destino el mismo móvil que lo ha originado), al cabo de un cierto tiempo se recibe el mensaje, por lo que aparece en el terminal lo siguiente:

```
+CMTI: "SM", 3
```

Que indica que se ha recibido un mensaje SMS y se ha almacenado con el número 3. Si ahora leemos el mensaje:

```
AT+CMGR=3
+CMGR: "REC UNREAD", "+34630672901", "05/06/23, 11:57:20+00"
Mensaje de prueba
OK
```

La información que se obtiene es la siguiente. Primero el estado del mensaje, “REC UNREAD”, para indicar que es un mensaje nuevo que no se había leído. A continuación el teléfono del remitente, la fecha y la hora en la que se ha recibido y finalmente el mensaje recibido. Si ahora se vuelve a leer el mensaje, el estado será “REC READ”. En caso de no haber cobertura a la hora de enviar el mensaje, el comando **AT+CMGS** devuelve la cadena **ERROR**.

```
AT+CMGS="630672901"<CR>
>Mensaje de prueba <control-z>
ERROR
```

Envío de un SMS en modo PDU

También es posible enviar directamente una trama SMS-SUBMIT. Para ello configuramos el módem para funcionar en **modo PDU**, con el comando **AT+CMGF=0** y después se utiliza el comando **AT+CMGS**, indicando la longitud de la trama (excluyendo el primer byte)

```
AT+CMGS=16 <CR>
> 000104098136602709F100F604686F6C61 <Control-z>
+CMGS: 8
OK
```

Si el primer byte es 00, no se envía información sobre el centro de mensajes, por lo que el módem toma el que tenga predefinido.

4.4 Módem GSM

4.4.1 Introducción

Actualmente están apareciendo gran cantidad de servicios basados en mensajes cortos. Además de ser usados para enviar mensajes de texto entre personas, de forma simular a los “busca”, se están ofreciendo otros servicios como son:

- Votaciones mediante SMS.
- Suscripción a servicios de información.
- Informe de averías en ciertos equipos. Por ejemplo, muchos cajeros automáticos envían un SMS al servicio técnico cuando detectan que hay alguna avería o les falta algún recurso: dinero, papel...
- Ofrecer servicios de soporte a otras empresas. Como la empresa Pulsar Technologies, que ofrece soporte con las impresoras de HP.

Para poder ofrecer estos servicios es necesario diseñar software y hardware que pueda acceder a los servicios SMS. Esto se puede conseguir de varias maneras:

1. Algunos teléfonos se pueden conectar directamente a un PC y mediante un software propietario se puede acceder a los datos de móvil (agenda, tarjeta SIM...), así como enviar y recibir mensajes SMS. El principal problema de esta solución es que no es abierta, y los fabricantes no proporcionan suficiente información como para poder realizar aplicaciones con ellos, siendo necesario realizar ingeniería inversa. No obstante, hemos de incidir en este punto que dada la profusión que esta alcanzando el mercado móvil en general y en nuestro país en particular, los fabricantes están intentando diversificar su mercado y es obvio que el mundo del hardware para telecontrol no les es ajeno. Es por esto que poco a poco la utilización de comandos AT y AT+ estándar se está generalizando.

No obstante, aún existen diferencias entre los terminales modernos de la llamada segunda generación, aunque atenuada en la llamada generación 2.5 (GSM+GPRS), sobre todo por la posibilidad que incorporan los terminales de

poder ser utilizados como módem. Otro problema remanente a esta solución es el interfaz hardware para estos terminales, pues no siempre es fácil encontrar en el mercado conectores adecuados para lograr el diálogo M2M (Machine-to-Machine). A pesar de todo lo indicado, se realizaron una serie de pruebas con un terminal Siemens S55 conectado al puerto serie de un PC y fue posible configurarlo y utilizarlo del mismo modo que el módem utilizado.

2. Utilización de un módem GSM, (es la solución adoptada). Mediante un módem GSM podemos conectar cualquier sistema digital a la red GSM, no sólo para enviar mensajes SMS sino también para transmitir datos. Existen dos tipos de módems, según la aplicación que queramos realizar.
 - a. módems para circuito impreso: Son módems de reducido tamaño (como una tarjeta de memoria aprox.) y perfectamente apantallados que están preparados para ser incorporados dentro de un circuito impreso y que permiten desarrollar un hardware específico y que no depende de un PC.
 - b. módems para PC. Fue la elección final, tienen un tamaño también bastante reducido, y disponen de un conector DB9 hembra para conectarse al PC a través de un cable serier. Son útiles para que desde cualquier ordenador de una intranet se puedan enviar mensajes SMS.

El módulo utilizado para el enlace radio a través de la red GSM ha sido el Eagle II de fabricante de equipos Xircom. Es un módulo pequeño, compacto y de tipo OEM que permite una comunicación y control bidireccionales y que es capaz de proporcionar la práctica totalidad de los beneficios que ofrece la red GSM:

- El uso de SIM (Subscriber Identification Module) proporciona ventajas como la portabilidad del número y actualizaciones remotas inalámbricas.
- La comunicación inalámbrica permite al módulo Eagle II cumplimentar tareas que previamente eran presenciales, esta capacidad ofrece nuevos e innovadores servicios para una aplicación.
- La autenticación del Terminal y la encriptación de datos que ofrece la red GSM asegura una comunicación confidencial entre el Terminal del usuario y el de datos.
- Una gran variedad de aplicaciones pueden emplear este módem para transmitir y recibir datos y voz como:
 - Lectura automática de medidas.
 - Verificación de tarjetas de crédito.
 - Acceso a correo electrónico e Internet.
 - Sistemas de gestión de flotas comerciales.
 - Telemática.
 - Telemetría.
 - Alarmas inalámbricas.

Además, el módulo provee de funcionamiento multibanda, con la banda de frecuencias seleccionable mediante comandos AT. Se ofrecen dos versiones distintas, una con las bandas 900/1900 MHz pensada para su utilización en América y otras regiones que utilicen la banda de 1900 MHz. El módulo del que se dispone, que cubre las bandas 900/1800 MHz, esta diseñado para el desarrollo de aplicaciones en Europa y el resto del mundo con la excepción del continente americano.

4.4.2 Incorporar la red GSM a un diseño

El módem seleccionado está diseñado para una fácil integración con otros componentes y las redes GSM existentes. Se comunica vía el interfaz serie V.24 y emplea el juego de comandos AT lo que le permite monitorizar la red y avisar de condiciones que puedan ser relevantes para la gestión de una red conformada por varios terminales.

El Eagle II soporta los siguientes servicios GSM:

- Servicio de mensajes cortos (SMS).
- Servicio suplementario de datos si estructurar (USSD).
- Servicio de conmutación de circuitos en modos transparente y no transparente para la transmisión y recepción de datos.
- Comunicación vocal, soporta los esquemas de codificación vocal half-rate, full-rate y enhanced full-rate (EFR).

4.4.3 Tabla de especificaciones del módem GSM

En la Tabla 4.1 se pueden ver resumidas las principales características del módulo GSM Xircom Eagle II.

Interfaz	Interfaz de entrada y salida de datos	60 pines, dos filas, 0,8 mm pitch SMD
	Puerto serie primario	Protocolo V.24, 3V nivel de tensión (soporta 5V)
	Puerto serie secundario	Algunas funciones que no sean el envío de SMS requieren el desarrollo de aplicaciones exproceso
	Voz	Soporta tres modos de codificación vocal: half-rate, full-rate y enhanced full-rate (EFR)
	Antena	Conector SMA RF hembra
	Protocolo de comandos	Juego de comandos AT
	Subscriber Identification Module (SIM)	Portadora e interfaz 3V mini-SIM on board
Power	SIM remoto opcional	Accesible a través del conector de 60 pines
	Alimentación eléctrica	Tensión continua fija
	Corriente de pico y disipación media	Consultar epígrafe siguiente
Interfaz radio	Bandas de frecuencia	Compatible con GSM 900 y DCS 1800
	Características GSM soportadas	Atenticación, encriptación y salto en frecuencia
Funcs. GSM	<ul style="list-style-type: none"> - Mensajes SMS Mobile-originates y mobile-terminated: hasta 140 bytes o 160 caracteres GSM ASCII de 7 bits. Hasta 255 mensajes se pueden concatenar. - Recepción de mensajes de difusión - Asentimiento de los mensajes recibidos - Encaminamiento por conmutación de circuitos (transparente o no a 9.6 Kbps) - Voz - Fax grupo 3 - Soporta GSM de fase 2+ - Soporta Servicio Suplementario de Datos no Estructurado (USSD) 	
IMEI	El IMEI (International Mobile Equipment Identity) permite desautorizar el uso a equipos robados o defectuosos	

Tabla 4.1 Resumen de características del módem GSM

Del mismo modo, en la Tabla 4.2 y la Tabla 4.3 se recogen las características técnicas fundamentales, para una consulta más exhaustiva, referirse al manual técnico del módem anexo.

- Potencia de funcionamiento:

Se requiere una entrada de tensión de 3.4 V DC a 4.0 V DC. El rizado en tensión debe ser inferior al 20% del valor medio de tensión bajo las condiciones normales de trabajo.

Eagle II (a 3.7 Voltios)		Intensidad Media	Intensidad de Pico
GSM 900	GSM	1 TX 1 RX	0.32 A
		1 RX	0.08 A
	GPRS Class 10	1 TX 4 RX	0.34 A
		2 TX 3 RX	0.58 A
	Sleep Mode	<20 mA	

DCS 1800 y PCS 1900	GSM	1 TX 1 RX	0.25 A	1.45 A
		1 RX	0.08 A	0.13 A
	GPRS class 10	1 TX 4 RX	0.27 A	1.45 A
		2 TX 3 RX	0.44 A	1.45 A
	Sleep Mode	<20 mA		

Tabla 4.2 *Potencia de funcionamiento*

- Potencia del transmisor:

Módulo Eagle II	Power class	Potencia transmitida
1900 MHz 1800 MHz	GPRS power class 1	1 W de potencia conducida ($30 \text{ dBm} \pm 2 \text{ dB}$), medidos en el puerto de la antena
900 MHz	GPRS power class 4	2 W de potencia conducida ($33 \text{ dBm} \pm 2 \text{ dB}$), medidos en el puerto de la antena

Tabla 4.3 *Potencia del transmisor*

- Sensibilidad del receptor:

La sensibilidad del receptor medida en el puerto de la antena es de -106 dBm como valor típico.

- Interfaz de antena:

El módulo Eagle II está diseñado para soportar tipos de antena intercambiables, supuesto que la antena tiene una impedancia de 50 Ohmios y está sintonizada en la banda de frecuencia adecuada. El módulo incorpora un conector para una antena de tipo SMA hembra, este tipo de conectores es preferible por su alta resistencia a las vibraciones, habituales en los entornos móviles.

4.4.4 Asignación de pines de entrada/salida

Se describen a continuación en la Tabla 4.4 la asignación de cada uno de los pines ordenados por funcionalidad. El número de pin se refiere a cada uno de los 60 pines del conector incorporado en la parte trasera del módulo. En el manual técnico se pueden consultar detalles referentes al tipo de conector recomendado para insertar en este terminal de entrada/salida.

Número de pin	Nombre de la señal	Dirección	Funcionalidad	Nivel de tensión
Alimentación				
1, 2, 3, 4, 5, 6	VIN	Del CPE	Entrada eléctrica al módulo, de 3.4 a 4.0 V DC.	
21, 24, 25, 28, 29,	GND	Del CPE	Retorno eléctrico para tierras analógicas y	

33, 44, 45, 48, 49, 52, 53, 57			digitales.	
Reset y canal serie primario				
23	RESET_B	Del CPE	Entrada de reset activa a nivel bajo, puede ser desconectada si no se usa. La duración del pulso mínima es 5 mS.	3 V
8	RX0	Al CPE	Receptor 0, señal de salida del DCE que se conecta al RX del DTE. A 1 lógico durante reset	3 V
16	TX0	Del CPE	Transmisor 0, señal de entrada del DCE nivel bajo que se conecta al TX del DTE. A 1 lógico durante reset	5 ó 3 V
18	CTS0	Al CPE	Clear To Send 0, señal de salida del DCE nivel bajo que se conecta al CTS del DTE	3 V
20	RTS0	Del CPE	Request To Send 0, señal de entrada del DCE nivel bajo que se conecta al RTS del DTE.	5 ó 3 V
22	DTR0	Del CPE	Data Terminal Ready 0, señal de entrada del DCE nivel bajo que se conecta al DTR del DTE.	5 ó 3 V
10	DSR0	Al CPE	Data Set Ready 0, señal de salida del DCE nivel bajo que se conecta al DSR del DTE.	3 V
12	DCD0	Al CPE	Data Carrier Detected 0, señal de salida del DCE nivel bajo que se conecta al DCD del DTE.	3 V
14	RI0	Al CPE	Ring Indicator 0, señal de salida del DCE nivel bajo que se conecta al RI del DTE.	3 V
Micrófono				
47	MIC1P	Del CPE	Entrada + de un micrófono. Tensión diferencial 2 V, impedancia mayor de 900Ω	
51	MIC1N	Del CPE	Entrada - de un micrófono. Tensión diferencial 2 V, impedancia mayor de 900Ω	
Altavoz				
55	SPK1P	Al CPE	Salida positiva de un altavoz de impedancia mínima 15Ω, capacidad 700pF y V _{pp} 4.5V	
59	SPK1N	Al CPE	Salida negativa de un altavoz de impedancia mínima 15Ω, capacidad 700pF y V _{pp} 4.5V	
Reloj				
27	CLKOUT	Al CPE	Salida de reloj cuadrada de 13 MHZ y duty cycle 50%. Para sincronización de circuitería exterior al procesador de banda base.	3 V
Entradas/salidas de propósito general				
13, 15, 17, 19	GPIO0-GPIO3	De/al CPE	Líneas de propósito general para monitorizar o controlar dispositivos externos	3 V
LEDs de estado				
40, 42	LED0-LED1	Al CPE	Activos a nivel bajo, se corresponden respectivamente al elemento rojo y verde de un LED bicolor. Indican el estado de la conexión radio	3 V
Líneas de datos de recepción y transmisión				
26	TX1	Al CPE	Transmisor 1, señal de salida secundaria del DTE usada para depuración y testeo	3 V
30	RX1	Del CPE	Receptor 1, señal de entrada secundaria del DTE usada para depuración y testeo	5 ó 3 V
Señales SIM				
58	SIM-VCC	Al CPE	Fuente de 3 V para un dispositivo de SIM remota. La controla por el procesador de banda base	3 ó 5 V
56	SIM-IN	Del CPE	Señal activa a nivel alto que indica la presencia de una tarjeta SIM remota	5 ó 3 V
54	SIM-RST	Al CPE	Señal de reset de una dispositivo de SIM remota	3 V

50	SIM-IO	AI/Del CPE	Línea para la comunicación serie con una SIM remota	5 ó 3 V
46	SIM-CLK	AI CPE	Señal de reloj a 3.25 Mhz para un dispositivo de SIM remota	3 ó 5 V
60	SIM-3V	AI CPE	Se usa junto con la señal SIM-IN en la conexión a un dispositivo de SIM remota	3 V
Estado				
7	TX on	AI CPE	Salida digital para indicar el estado de la fuente del transmisor, activa a nivel alto	2.2 V
9	RX on	AI CPE	Salida digital para indicar el estado de la fuente del emisor, activa a nivel alto	2.2 V
Reservado				
11, 31, 32, 34, 35, 36, 37, 38, 39, 41, 43	Reservado		Dejar sin conectar	

Tabla 4.4 *Asignación de pines del módem*

4.4.5 Indicador de estado

El módem utilizado dispone de un LED multicolor que indica el estado del enlace en tiempo real y la calidad de la señal, en la Tabla 4.5 se detalla la casuística.

Color	Estado del enlace	Calidad de la señal
Verde	El módulo esta conectado a la red	La señal es óptima
Naranja		El enlace no llega a ser óptimo pero es aceptable
Rojo fijo		La conexión es inaceptable
Rojo intermitente	El módulo esta en fase de inicialización o no hay conexión a la red	

Tabla 4.5 *Indicador de estado*

4.4.6 Modos de funcionamiento

La red GSM provee de numerosos servicios y modos de operación opcionales. El módulo Eagle II proporciona los siguientes servicios GSM:

- Comunicación vocal.
- Transmisión de datos por circuito conmutado.
- Servicio de mensajes cortos (SMS).
- Fax grupo 3.
- General Packet Radio Service (GPRS):

Recordemos que cada servicio GSM dispone de dos modos que pueden ser habilitados independientemente:

- Mobile-Originated (MO): permite hacer una solicitud de servicio como puede ser hacer una llamada o enviar un SMS.
- Mobile-Terminated (MT): Permite recibir la respuesta de un servicio como puede ser recibir una llamada o un SMS.

4.4.6.1 SMS: Short Message Services

El módulo Eagle II puede efectuar las siguientes tareas:

- Enviar y recibir mensajes binarios de hasta 160 caracteres de 7 bits.
- Enviar y recibir mensajes de texto de hasta 140 bytes.
- Remitir un SMS Unidad de Datos de Protocolo (PDU) a un centro del servicio de mensajes cortos SMSC y almacenar una copia de la PDU hasta que llegue un aviso de la red o expire un temporizador.
- Recibir un SMS PDU del SMSC.
- Recibir un informe de la red.
- Devolver un aviso de reparto de la red que previamente recibió el mensaje.
- Nidificar a la red cuando el módulo tiene capacidad de memoria suficiente para recibir uno o más mensajes SMS (después de que el módulo haya rechazado previamente un mensaje porque su capacidad fue excedida).
- Soporta Mobile-Originated y Mobile-Terminated SMS.
- Envio del mensaje a un teléfono.
- Soporta 8 bits de datos.
- Soporta mensajes de clase 1.
- Permite la concatenación de hasta 255 mensajes.
- Provee de un indicador de avisos de estado.
- Permite la definición de un periodo de validez.
- Provee al Service Center Time Stamp.
- Alerta al SMSC.

- Permite prioridad.
- Permite mensajes en espera.
- GPRS.

4.4.7 Interfaz software del módulo Eagle II

La aplicación que se comunique con el módem a través del conector de 60 pines emplea el juego de comandos AT+. Ello le permite operar en uno de los siguientes modos:

- Modo comando: Utilizado para configurar el módem, para consultar algo a la red GSM y para hacer y recibir llamadas. Para hacerlo, los comandos se envían por el canal serie de comunicación.
- Modo on-line: Utilizado una vez que el circuito está establecido, los datos pasan del módem a la aplicación de control sin interpretación de comandos. El único comando AT que es interpretado en modo on-line es el comando +++, que devuelve al módem a modo comando (ahora puede recibir cualquier comando), pero sin terminar la llamada por conmutación de circuitos que está establecida.

En modo comando, los caracteres que se reciben del CPE (Customer Premise Equipment) se tratan como comandos AT por parte del módem. Del mismo modo, en respuesta a los comandos recibidos del CPE, el módem envía caracteres (comandos AT) al CPE. Existen igualmente eventos como la inicialización del módem que envían comandos AT al CPE sin solicitud previa por parte de éste.

4.4.8 Interfaz hardware del módulo Eagle II

En la sección 4.4.4 Asignación de pines de entrada/salida, página 87, se indica la relación de pines que se dispone en el módem escogido y se puede comprobar que es tremadamente versátil. Sin embargo, para disponer de estas funcionalidades, necesitamos conectar dicho módem con la placa que diseñemos utilizando un conector adecuado y, las reducidas dimensiones de éste, 22 mm. aprox, nos hicieron buscar una alternativa más viable. La solución adoptada fue adquirir una tarjeta adaptadora que incluye el citado conector y dispone de una entrada para alimentar al bloque módem-tarjeta adaptadora y un conector db9 hembra para permitir la comunicación con el módem según la norma RS-232. Hemos conseguido un interfaz hardware mucho más amigable pero a costa de ver mermada considerablemente las funcionalidades del módem y el evidente desembolso económico.

Un problema fundamental de esta merma es que perdemos la funcionalidad de reset hardware que estaba disponible a través del pin 23 del citado conector, el hecho de no existir tampoco una orden hardware similar nos obligó a diseñar un interruptor basado en un transistor MOSFET controlable desde el microcontrolador que fuese capaz de gobernar la alimentación de la placa y, a través de esta, del módem.

Otro de los problemas que trajo aparejados la inclusión de la tarjeta adaptadora en el diseño fue que el distribuidor no proporcionaba ninguna documentación relativa al mismo, véanse tensiones de alimentación, consumos de intensidad y potencia, regímenes binarios soportados por el interfaz para transmisión serie, etcétera. Estas dificultades complicaron el diseño de la fuente de alimentación del módem, siendo necesario utilizar “ingeniería inversa” para comprender qué niveles de tensión eran los adecuados. La placa cuenta con un regulador de tensión de la familia 8015, que nos lleva a alimentar al sistema provisionalmente con 12 Vdc suministrados por una fuente de alimentación de PC por disponer este tipo de fuentes del conector adecuado para el adaptador, si bien es posible alimentar al equipo con tensiones inferiores, del orden de 7.5 Vdc. Este aspecto se reveló de suma importancia en las fases intermedias del diseño, pues en una primera etapa no se incluyó el interruptor capaz de reiniciar al módem y, a pesar de que se intentó depurar su diseño al máximo, su inclusión provocaba que la tensión de alimentación cayese hasta los 10 Vdc por el consumo de dicho interruptor. En la Figura 4.9, se aprecia el anverso del sistema montado, y en la Figura 4.10 aparece el reverso.



Figura 4.9 Módem GSM más placa adaptadora (anverso)

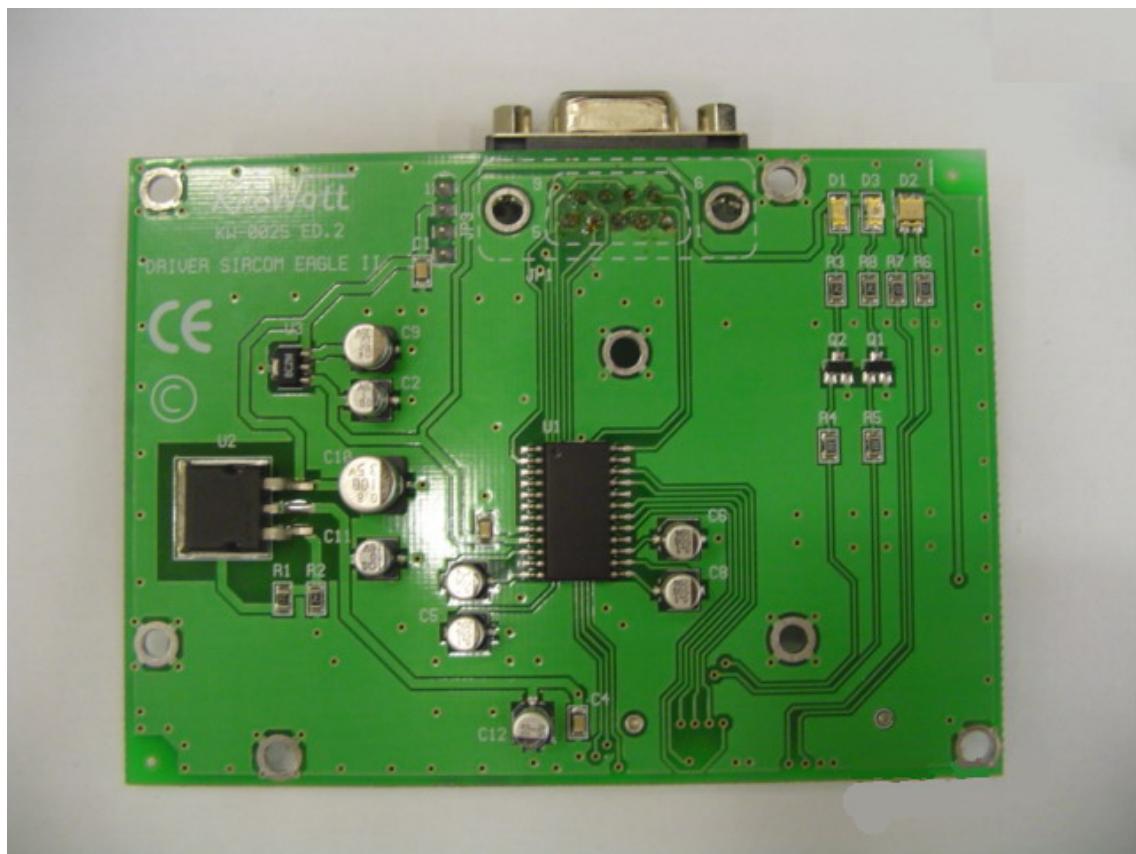


Figura 4.10 Módem GSM más placa adaptadora (reverso)