

EL SERVICIO SMS: UN ENFOQUE PRACTICO

Juan González Gómez

**Trabajo de doctorado de la asignatura
"Nuevas tecnologías para las comunicaciones"**

Curso 2001/02

**Escuela Técnica Superior de Ingeniería Informática
UAM**

Página en blanco

EL SERVICIO SMS: UN ENFOQUE PRÁCTICO

Juan González Gómez

27/Junio/2002

Trabajo de doctorado para la asignatura “Nuevas tecnologías para las comunicaciones”.
Impartida por los profesores:

- D. Javier Martínez Rodríguez
 - D. Francisco Gómez Arribas
 - D^a Susana Holgado González-Guerrero
 - D. Luis de Pedro Sánchez
-

Resumen

El servicio de mensajes cortos, SMS, está teniendo un gran auge en nuestros días, y está siendo mucho más utilizado de lo que inicialmente se estimó. En este trabajo se describe el servicio SMS desde un punto de vista práctico, haciendo hincapié en cómo es posible realizar aplicaciones que utilicen este servicio. Se parte de una descripción teórica de la red GSM en general y del servicio SMS en particular para familiarizarse con la terminología y tener una idea básica de lo que está pasando por debajo. Se describen los protocolos necesarios, centrándose en la capa de transferencia de mensajes, que es la que se utiliza desde las aplicaciones. Se muestra cómo es la interfaz entre las aplicaciones y el servicio SMS utilizándose un módem GSM para tener acceso a ellas, y cómo es posible controlar este módem mediante los comandos AT y AT+. Finalmente se muestra un ejemplo de una aplicación, gterm, muy sencilla, que permite enviar mensajes, leerlos, borrarlos, listar los teléfonos, etc. Se trata de una aplicación básica a partir de la cual se pueden realizar programas mucho más complejos.

Página en Blanco

Índice

1. Introducción	9
2. Introducción a GSM	9
2.1. Servicio	9
2.2. Arquitectura de red GSM	9
2.3. Sistema celular	11
2.4. Interfaz Radio (Um)	13
3. SMS	13
3.1. Servicio SMS	13
3.2. Arquitectura de red	14
3.3. Nivel SM-TL y protocolo SM-TP	15
3.3.1. SMS-SUBMIT	19
3.3.2. SMS-DELIVER	20
3.3.3. Un ejemplo de trama SMS-SUBMIT	21
4. Acceso a los servicios SMS	22
4.1. Introducción	22
4.2. Interfaz con MODEMS: comandos AT	24
4.3. Interfaz con Modems GSM	26
4.3.1. Comandos AT+	26
4.3.2. Algunos ejemplos	28
5. Construcción de una aplicación de acceso a los servicios SMS	32
5.1. Introducción	32
5.2. Plataforma	32
5.2.1. Plataforma hardware	32
5.2.2. Plataforma Software	33
5.3. Descripción de la aplicación	33
5.4. Utilización de Gterm	34
5.4.1. Conexión inicial	34
5.4.2. Listando teléfonos y mensajes	37
5.4.3. Lectura y borrado de un sms	37
5.4.4. Envío de un mensaje	37
5.5. Listado de la aplicación	37
5.5.1. Módulo serie.c	37
5.5.2. Módulo interface.c	40
5.5.3. Programa principal: gterm.c	41
6. Conclusiones	42

<i>ÍNDICE</i>	6
7. Líneas futuras	43
8. Glosario de términos	44

Índice de figuras

1.	Arquitectura de red GSM	10
2.	Sistema Celular	12
3.	Tramas TDMA y SLOTS	13
4.	Servicio SMS	14
5.	Envío de un SMS entre una MS y una entidad fija	15
6.	Servicios básicos SM MT y SM MO	16
7.	Estructura básica de la red para la transferencia de mensajes cortos	17
8.	Niveles y servicios para el envío de mensajes cortos	17
9.	Las 6 PDUs del SM-TP	18
10.	Trama SMS-SUBMIT	20
11.	Detalle del campo SCA	20
12.	Trama SMS-DELIVER	21
13.	Trama SMS-SUBMIT de ejemplo	22
14.	Utilización de un módem GSM desde un sistema digital	23
15.	Tarjeta DACER, con un módem GSM integrado	24
16.	Un módem GSM para PC	25
17.	Conexión entre un Módem y un PC	26
18.	Diagrama de bloques de gterm	34
19.	La aplicación gterm	35
20.	Partes que componen el interfaz de Gterm	36
21.	Ejecución inicial de Gterm	38
22.	Lectura/borrado de mensajes	39
23.	Envío de un SMS	39

Página en Blanco

1. Introducción

En este trabajo se describe el servicio SMS, desde un punto de vista práctico, enfocado al desarrollo de aplicaciones basadas en él. La estructura del trabajo es la siguiente:

En el **apartado 2** se describe brevemente el **sistema GSM** y la arquitectura de red subyacente. Se puede encontrar más información en la documentación proporcionada en el curso de doctorado “Nuevas tecnologías para comunicaciones”[2], en el libro de texto [3] y en la web de la ETSI[1].

En el **apartado 3** se describe el **servicio SMS** así como la arquitectura de red y los protocolos empleados, centrándose en el **protocolo SM-TP**, que es el que utiliza el nivel de aplicación para enviar/recibir mensajes cortos. Más información se puede encontrar en [4].

El **apartado 4** se dedica al interfaz entre la aplicación y el **módem GMS**, describiéndose brevemente los **comandos AT** y **AT+**. Se puede encontrar mucha información en la web, realizándose la búsqueda indicada en [5]. Algunas webs interesantes para los comandos AT [6, 7]. Un documento de referencia excelente es el proporcionado por Wavecom [8].

En el **apartado 5** se describe la **aplicación Gterm**, realizada para mostrar el manejo de los modems GSM, desde un punto de vista práctico, que permita al lector realizar aplicaciones más avanzadas. Se muestran los listados de los módulos al final del apartado.

Finalmente en el 6 se extraen las conclusiones y en el 7 se muestran las líneas futuras para la continuación de este trabajo.

Puede resultar útil el glosario de términos que se encuentra en el **apartado 8**.

2. Introducción a GSM

2.1. Servicio

GSM (Global System for Mobile Communication) es un sistema de comunicaciones móviles que ofrece los siguientes **servicios**:

- Transmisión/recepción de voz
- Transmisión/recepción de datos
- Envío/recepción de mensajes cortos (Sort Message Service, SMS)

2.2. Arquitectura de red GSM

En la figura 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 este trabajo es describir el servicio SMS a nivel de aplicación, sin entrar en demasiados detalles de la red subyacente.

La arquitectura GSM está constituida por tres partes:

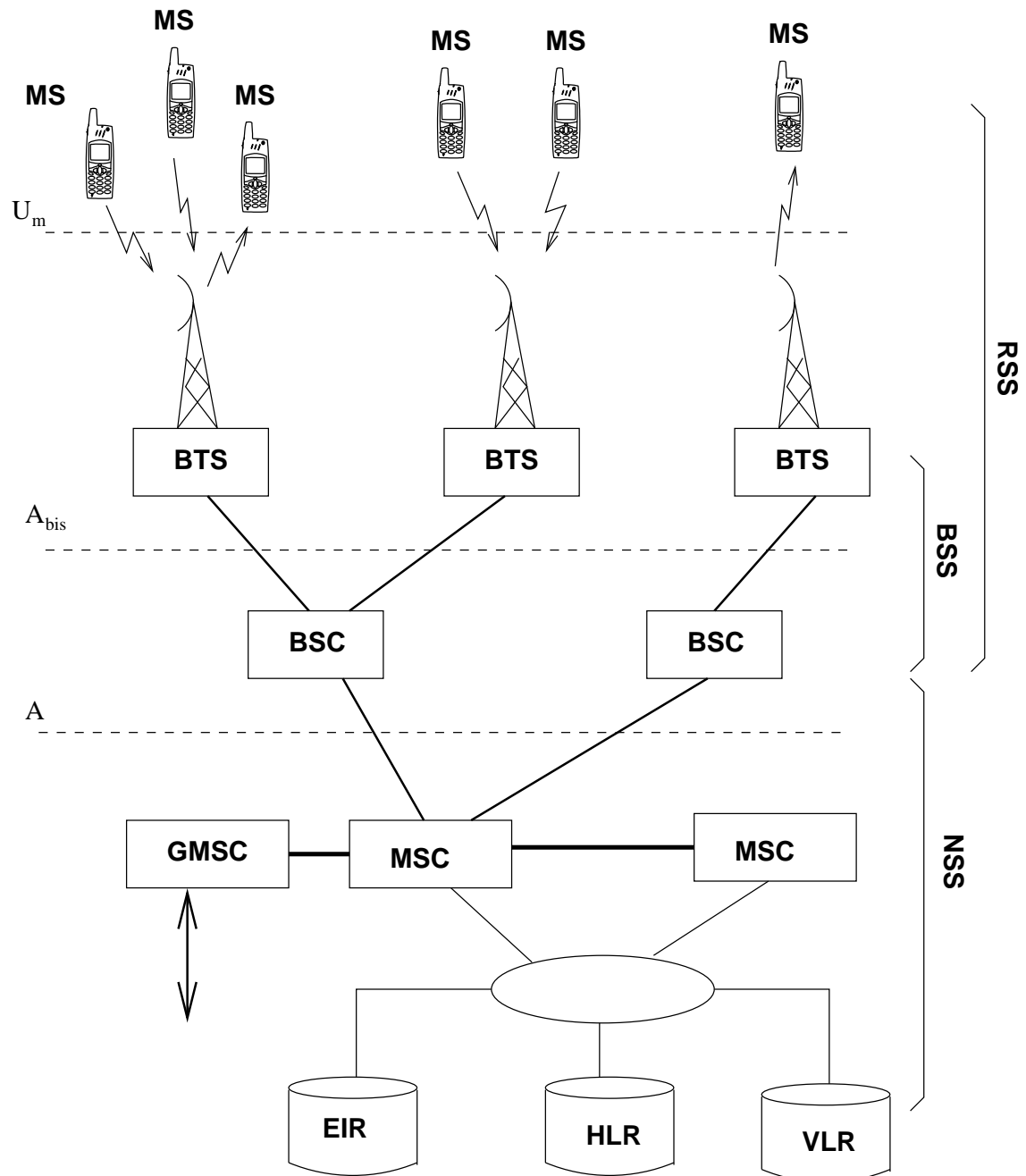


Figura 1: Arquitectura de red GSM

1. **Subsistema Radio (RSS, Radio SubSystem)**. Cubre la comunicación entre las estaciones móviles (**MS**) y las estaciones base (**BS**). El interfaz radio entre ellas se denomina U_m .
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 U_m).
 - 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 16kbts/s (A_{bis}) y por otro lado se comunica con los **MSC** a través del interfaz A, con canales de 64kbts/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**:
 - 1) **HLR (Home Location Register)**
 - 2) **VLR (Visitor Location Register)**
 - 3) **EIR (Equipment Identity Register)**

2.3. Sistema celular

El sistema GSM está basado en una *arquitectura celular* que permite una mejor utilización del espectro a base de replicar unas unidades fundamentales o celdas, con las que se tesela el área que se quiere cubrir. El tamaño de las celdas es un parámetro de diseño que se calcula en base al número medio de usuarios (tráfico medio generado) y el porcentaje de utilización de la estación base. Cuanto menor sea el radio de las celdas, mayor cantidad de usuarios puede soportar el sistema, sin embargo mayor es el coste en infraestructura.

En las ciudades el radio es pequeño (100m-1Km) mientras que en las zonas menos pobladas el radio es mayor, cubriéndose con una única estación base una mayor superficie (Hasta 30Km por celda).

En la figura 2 se muestra un ejemplo de un trozo de un sistema celular, en el que las células tienen el mismo tamaño. Todas las estaciones base (**BS**) están interconectadas a través del subsistema de red (**NSS**).

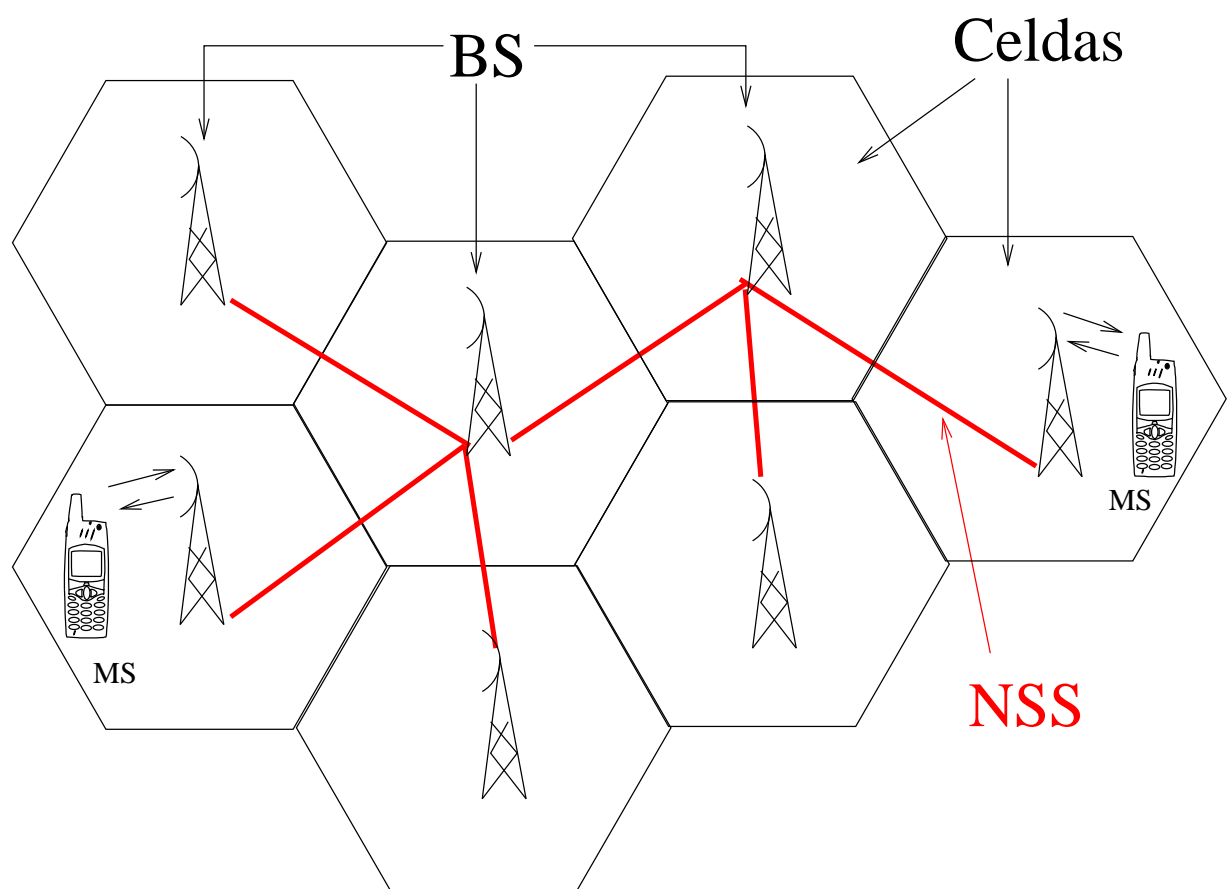


Figura 2: Sistema Celular

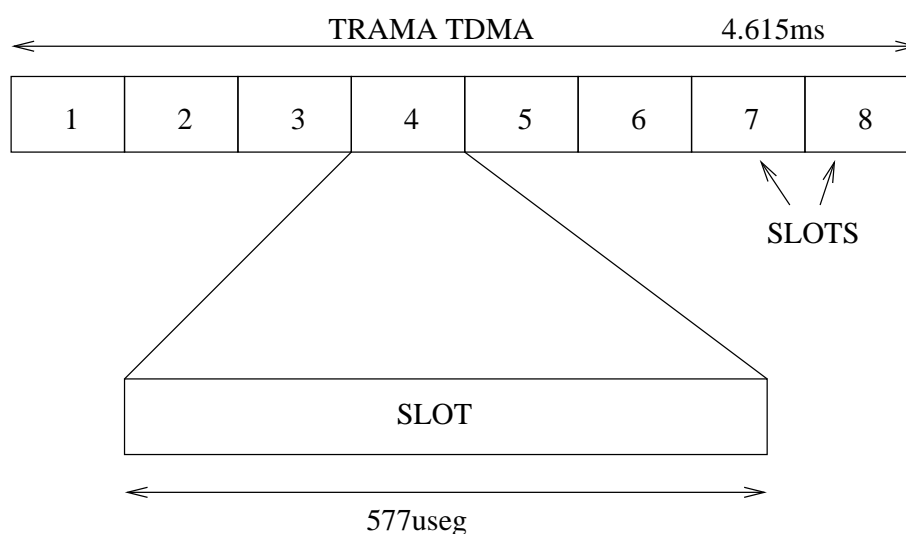


Figura 3: Tramas TDMA y SLOTS

2.4. Interfaz Radio (Um)

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 se multiplexan en el tiempo 8 ranuras, formando una trama TDMA. (Figura 3)

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.**

3. SMS

3.1. Servicio SMS

El **servicio SMS** permite transferir un mensaje de texto entre una estación móvil (**MS**) y otra entidad (**SME**) a través de un centro de servicio (**SC**) (Figura 4)

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 (o realizar alguna votación, sobre todo en los concursos de la TV, que ahora están tan de moda), un extremo es una estación móvil y la otra es un servidor que atiende las peticiones (o anota los votos).

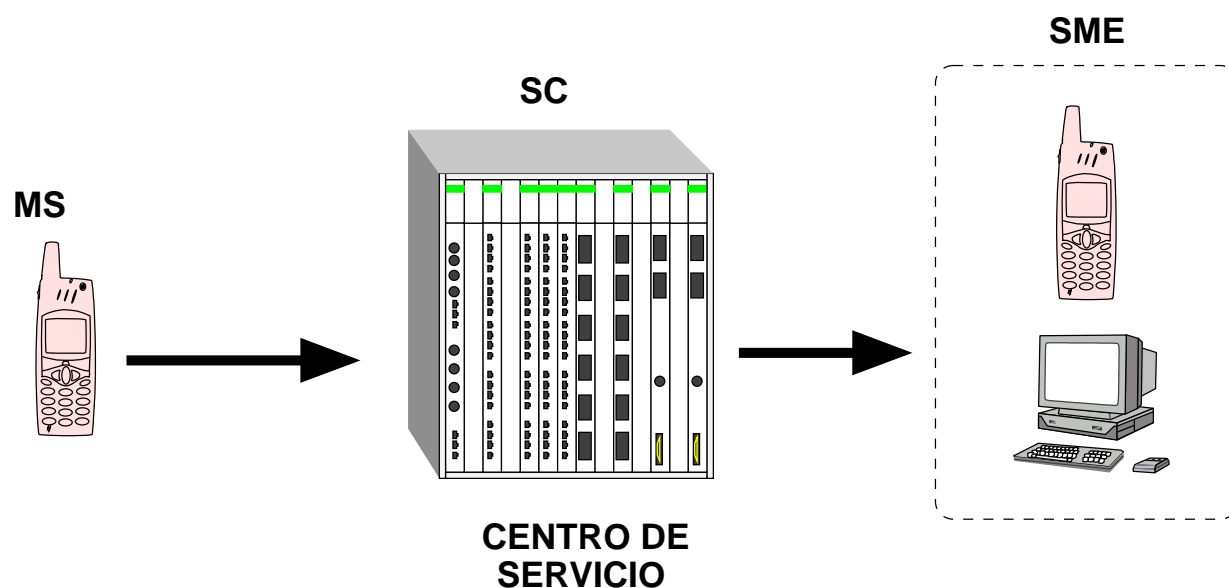


Figura 4: Servicio SMS

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 5).

El servicio SMS se divide en dos servicios Básicos (figura 6):

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.

3.2. Arquitectura de red

La estructura básica de la red para el servicio SMS se muestra en la figura 7. Las entidades involucradas son las siguientes:

- **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**

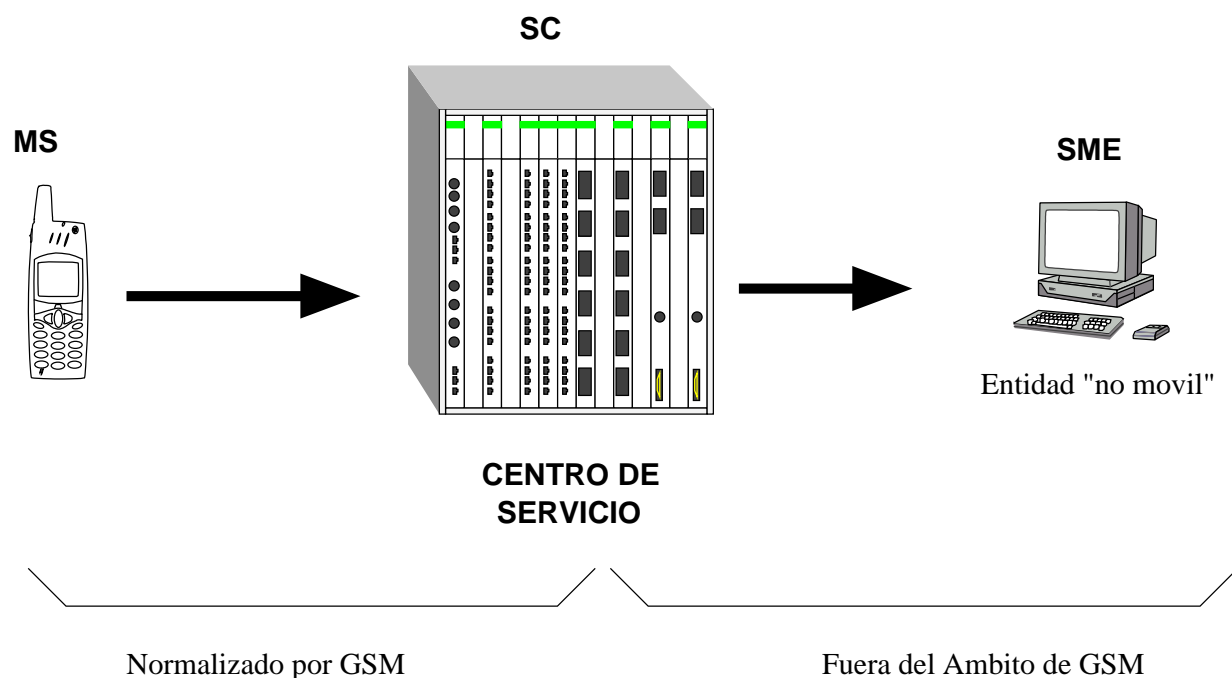


Figura 5: Envío de un SMS entre una MS y una entidad fija

Para la descripción detallada de la arquitectura, se utiliza un modelo de capas, 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(Figura 8):

- **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.**

3.3. Nivel SM-TL y protocolo SM-TP

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 de este trabajo es el **SM-TL**, que es el que se usará para enviar y recibir SMS.

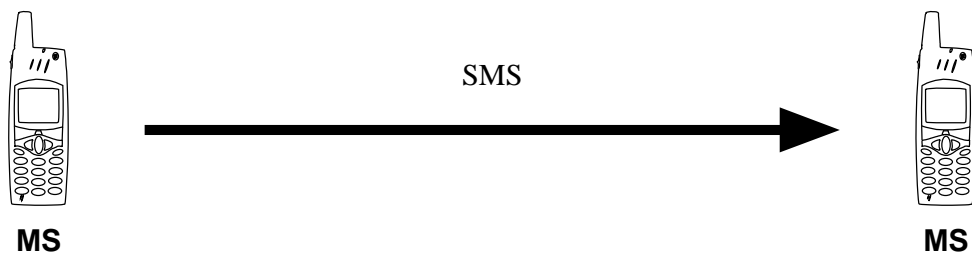
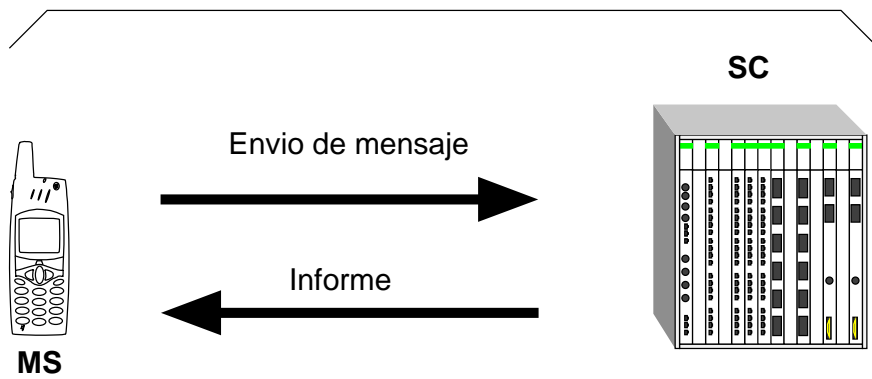
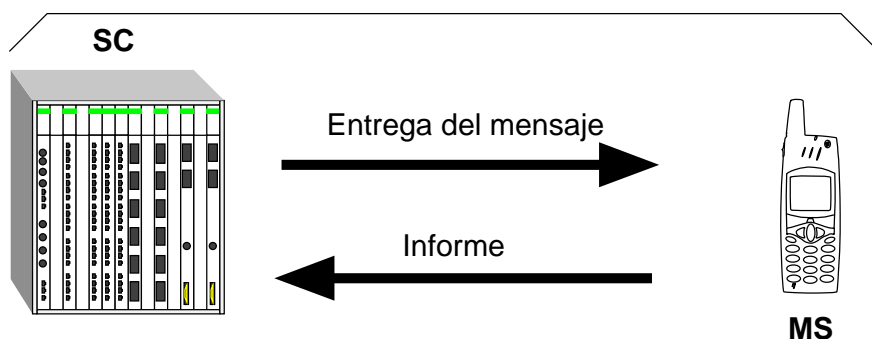
Servicio SMS entre dos MS**1) Servicio SM MO****2) Servicio SM MT**

Figura 6: Servicios básicos SM MT y SM MO

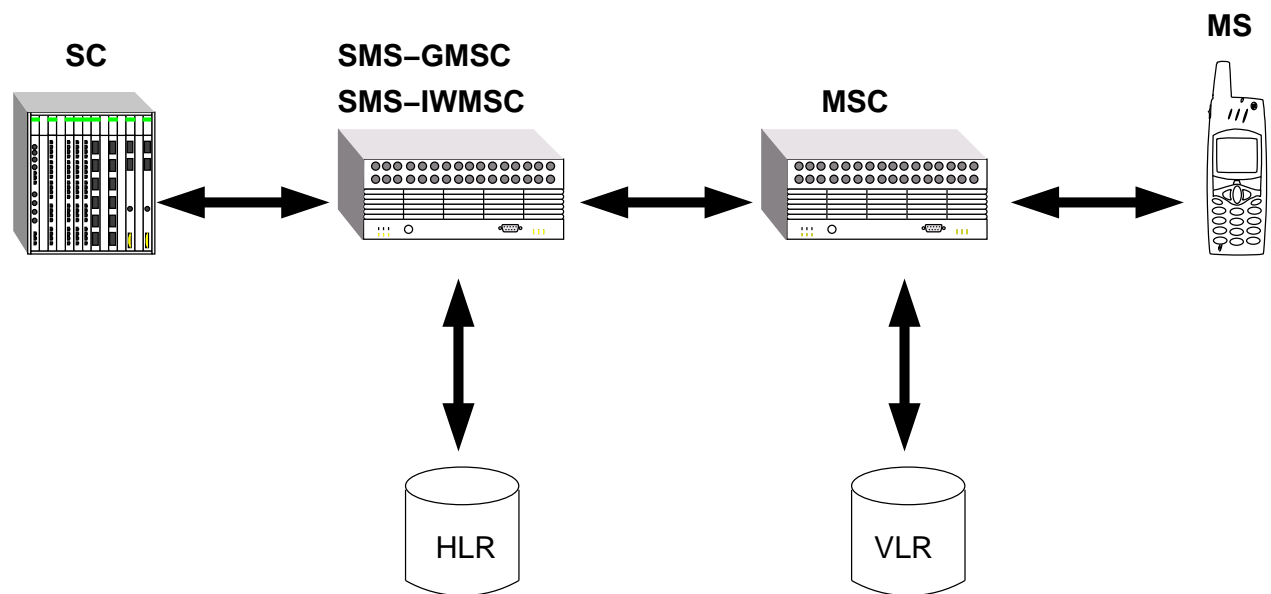


Figura 7: Estructura básica de la red para la transferencia de mensajes cortos

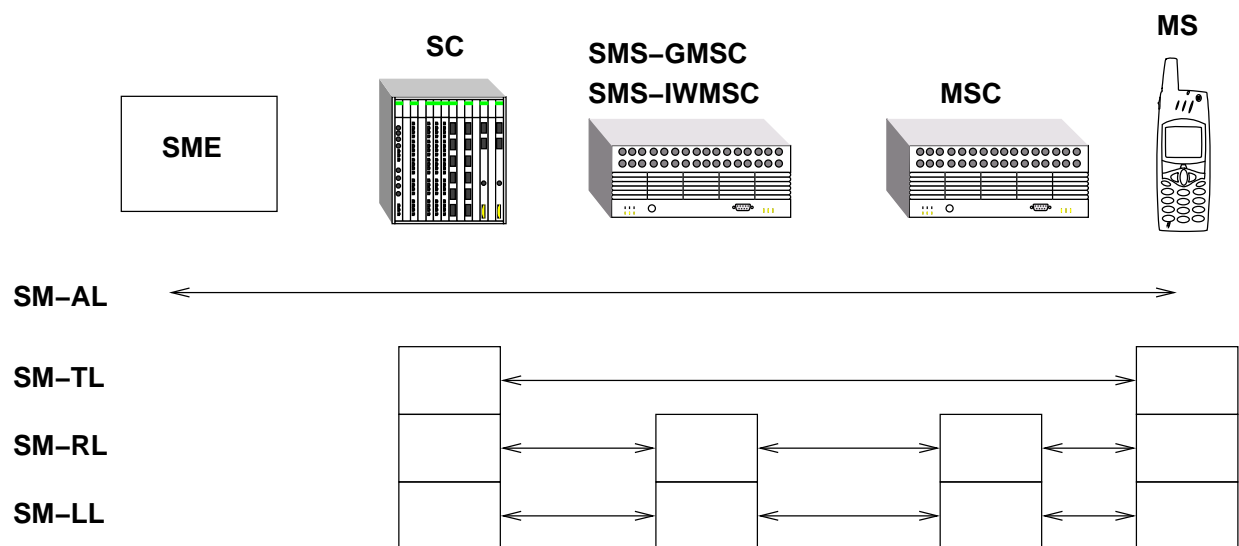


Figura 8: Niveles y servicios para el envío de mensajes cortos

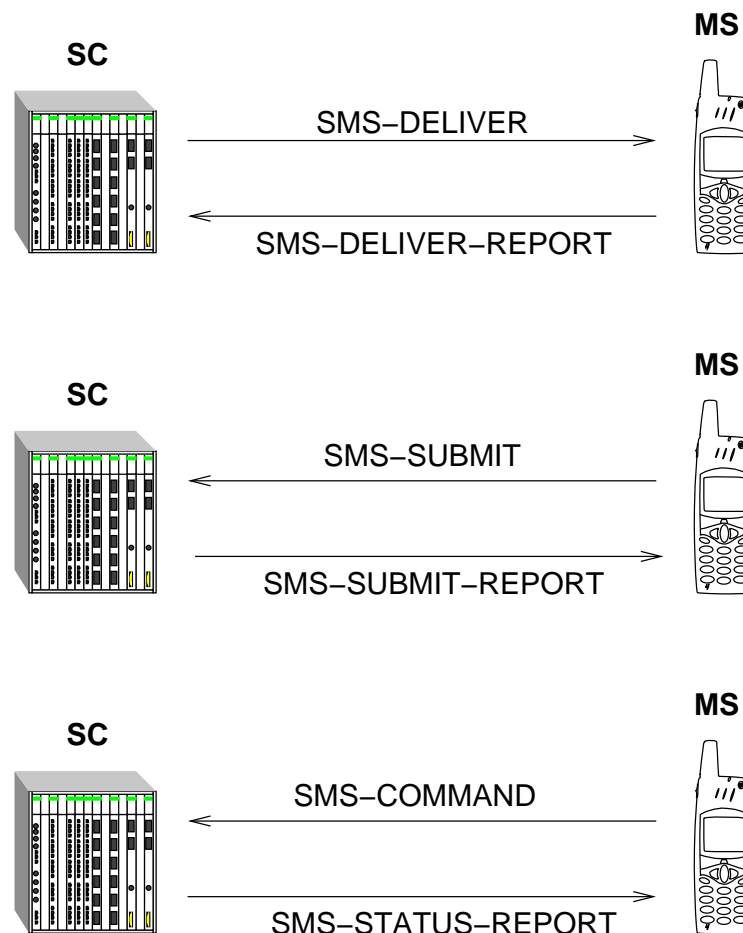


Figura 9: Las 6 PDUs del SM-TP

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.

Se utilizan las siguientes 6 PDUs (Figura 9):

- **SMS-DELIVER:** Transmitir un mensaje desde el **SC** al **MS**
- **SMS-DELIVER-REPORT:** Error en la entrega (si lo ha habido)
- **SMS-SUBMIT:** Transmitir 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**

3.3.1. SMS-SUBMIT

La estructura de la PDU **SMS-SUBMIT** se muestra en la figura 10. 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 11. 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:

Bit 1	Bit 0	Descripción
0	0	SMS-DELIVER
0	0	SMS-DELIVER-REPORT
0	1	SMS-SUBMIT
0	1	SMS-SUBMIT-REPORT
1	0	SMS-STATUS_REPORT
1	0	SMS-COMMAND
1	1	Reservado

- **MR**: Parámetro para identificar el mensaje
- **DA**: Dirección del SME destino (número de tlf)
- **PID**: Identificación del protocolo de la capa superior
- **DCS**: Identificación del tipo de codificación dentro de los datos de usuario

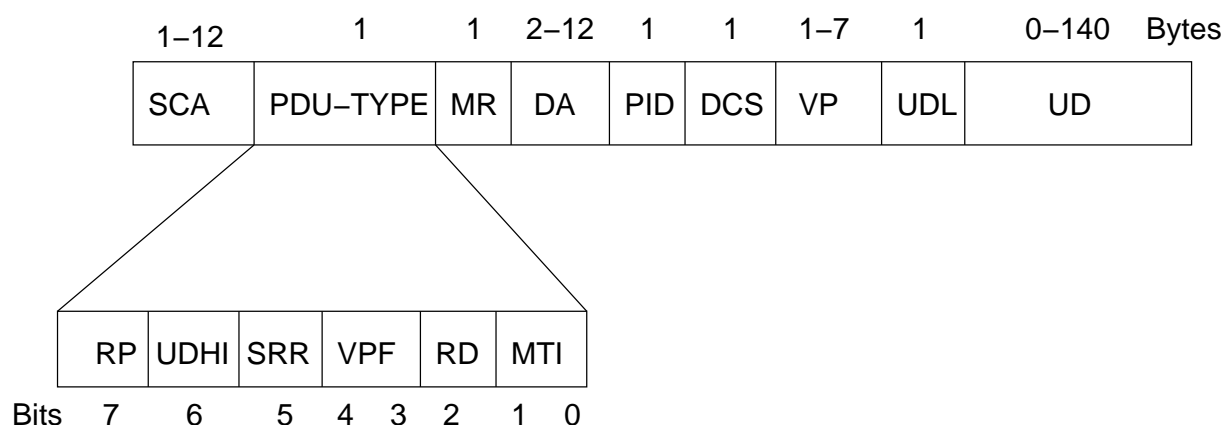


Figura 10: Trama SMS-SUBMIT

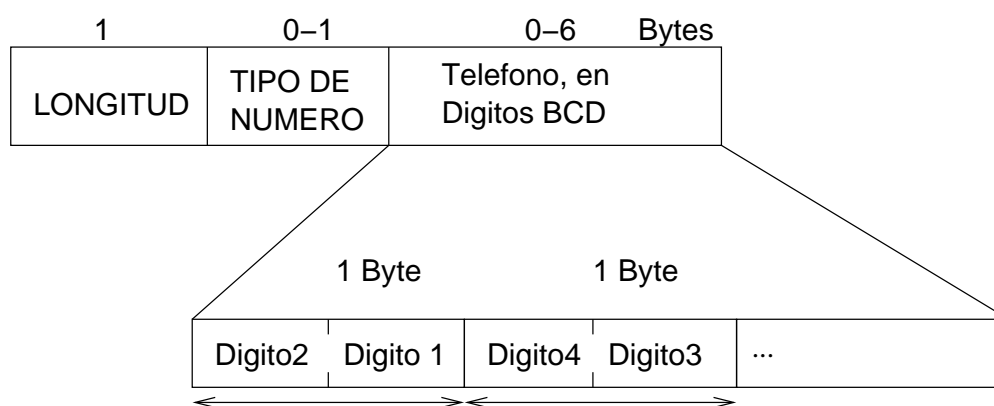
SCA

Figura 11: Detalle del campo SCA

- **VP:** Periodo de validez del mensaje
- **UDL:** Longitud del campo **UD**
- **UD:** Datos de usuario

3.3.2. SMS-DELIVER

Esta trama, transmitida desde el **SC** hasta el **MS**, tiene una estructura similar a **SMS-SUBMIT** y se muestra en la figura 12.

Los nuevos campos que aparecen son los siguientes:

- **OA:** Dirección del SME que envía el mensaje
- **SCTS:** Marca de tiempo de cuando el centro de servicio recibió el mensaje

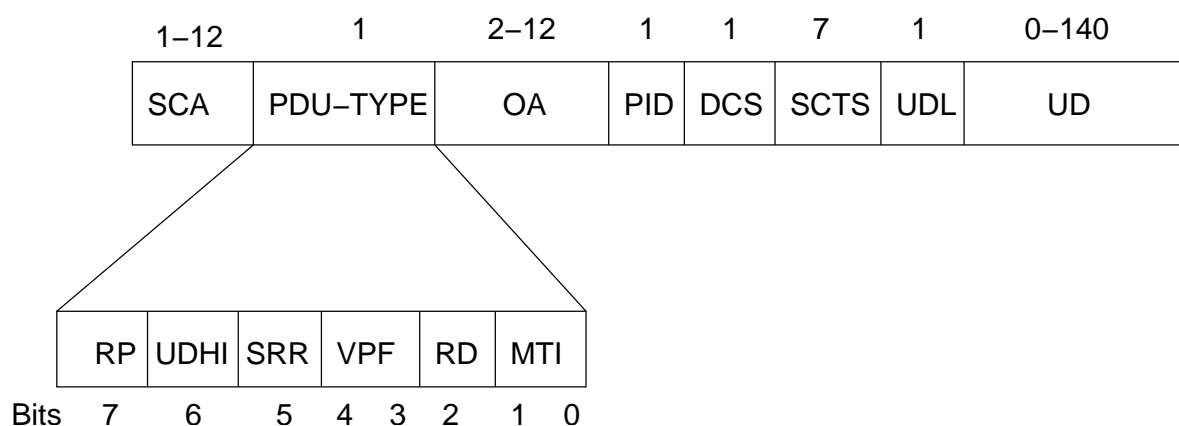


Figura 12: Trama SMS-DELIVER

3.3.3. Un ejemplo de trama SMS-SUBMIT

Se quiere 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.

7	6	5	4	3	2	1	0
RP	UDHI	SRR	VPF	RD	MTI		
0	0	0	0	0	0	1	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	l	a
68	6F	6C	61

La trama final es la mostrada en la figura 13, que ocupa 24 bytes.

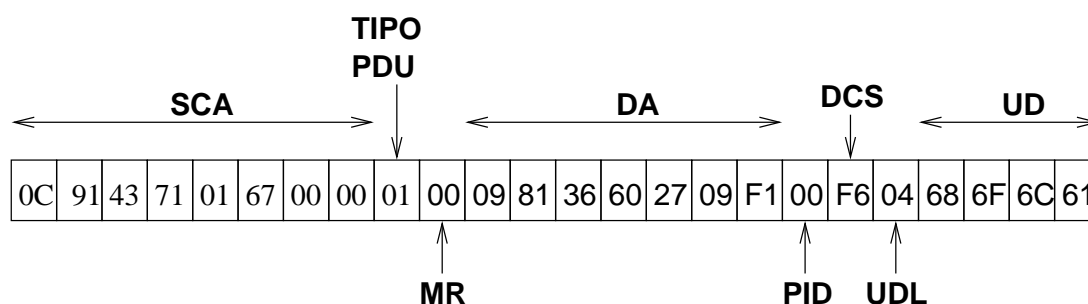


Figura 13: Trama SMS-SUBMIT de ejemplo

4. Acceso a los servicios SMS

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 similar a los “busca”, se están ofreciendo otros servicios como son:

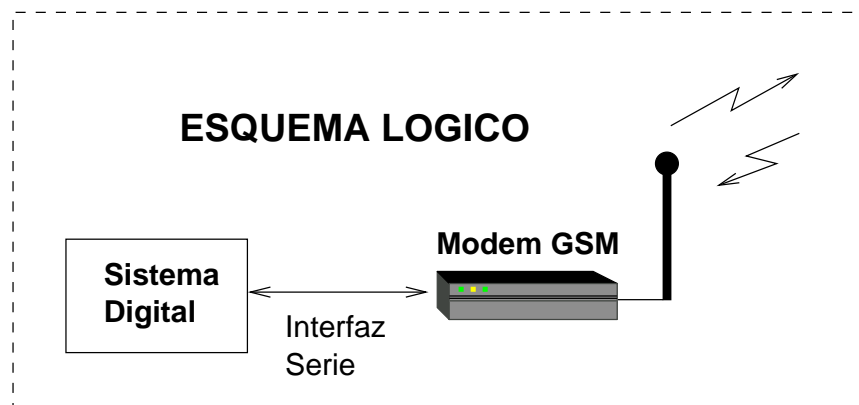
- Votaciones mediante SMS
- Suscripción a servicios de información, como por ejemplo el ofrecido durante estos mundiales, que te envían un SMS cada vez que la selección Española marca un gol.
- Informe de averías en ciertos equipos. Por ejemplo, muchos cajeros automáticos envían un SMS al servicio técnico 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[9].

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 fabricante no proporcionan suficiente información como para poder realizar aplicaciones con ellos. Es necesario realizar ingeniería inversa.
2. Utilización de un **MÓDEM GSM**. Esta es la solución empleada en este trabajo.

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 MODEMS, según la aplicación que queramos realizar (Figura 14.



IMPLEMENTACIONES

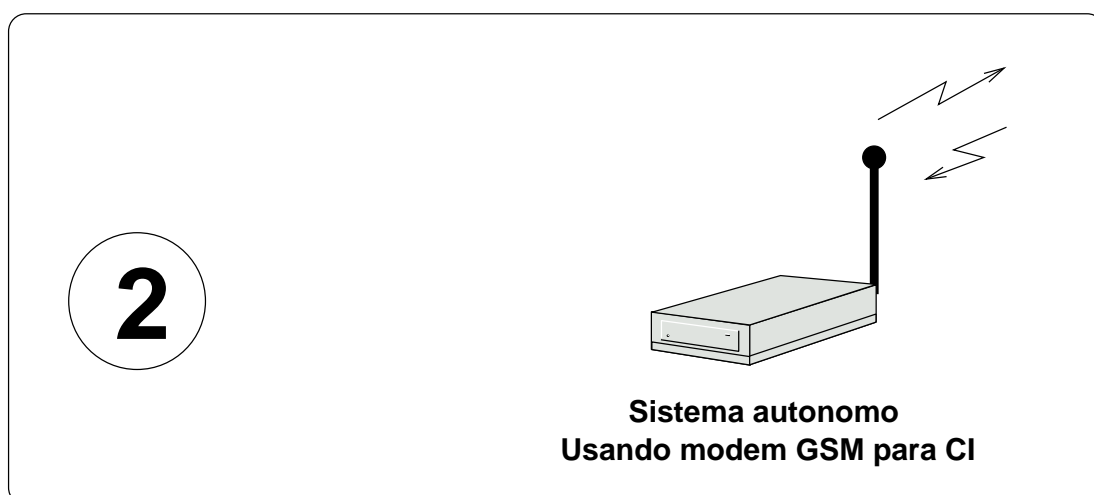
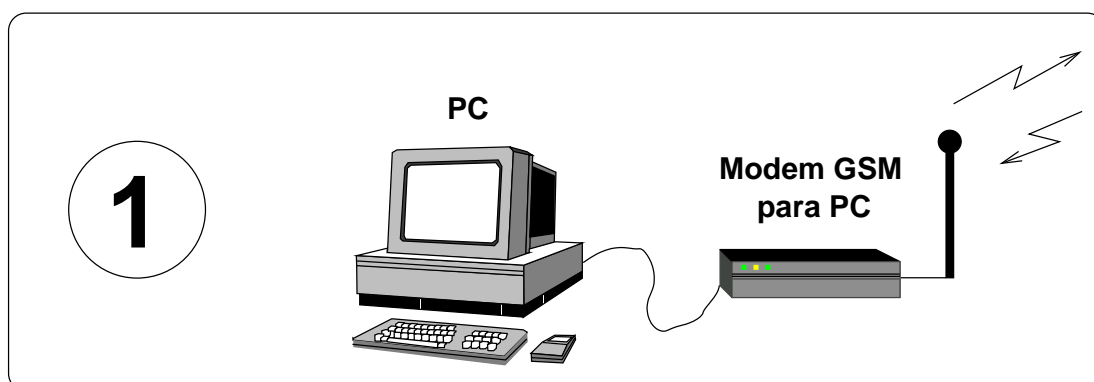


Figura 14: Utilización de un módem GSM desde un sistema digital

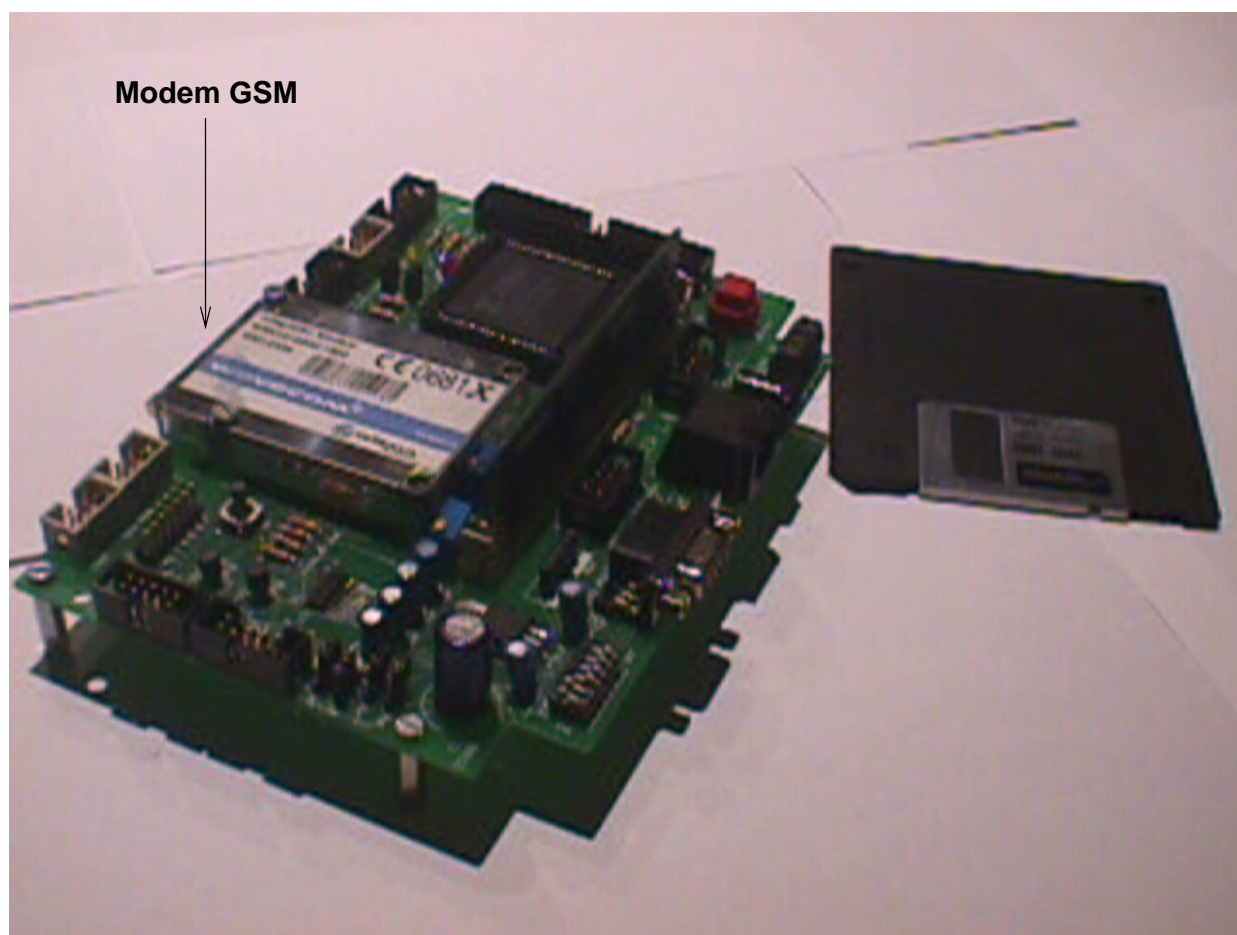


Figura 15: Tarjeta DACER, con un módem GSM integrado

1. **MODEMS para circuito impreso:** Son Modems de reducido tamaño 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. En la figura 15 se muestra la tarjeta DACER, desarrollada para la empresa Pulsar Technologies, que incorpora un módem GSM para circuito impreso. Obsérvese el tamaño del módem en comparación con el disquete.
2. **MODEMS para PC.** Tienen un tamaño también bastante reducido, y disponen de un conector DB9 hembra para conectarse al PC a través de un cable serie estándar. Son muy útiles para permitir que desde cualquier ordenador de una intranet se puedan enviar mensajes SMS (Ver figura 16).

4.2. Interfaz con MODEMS: comandos AT

La comunicación con los Modems se realiza a través de una **línea serie**, y dependiendo del módem, se pueden usar los niveles definidos por la **norma RS232** (Modems para PC) o **niveles**

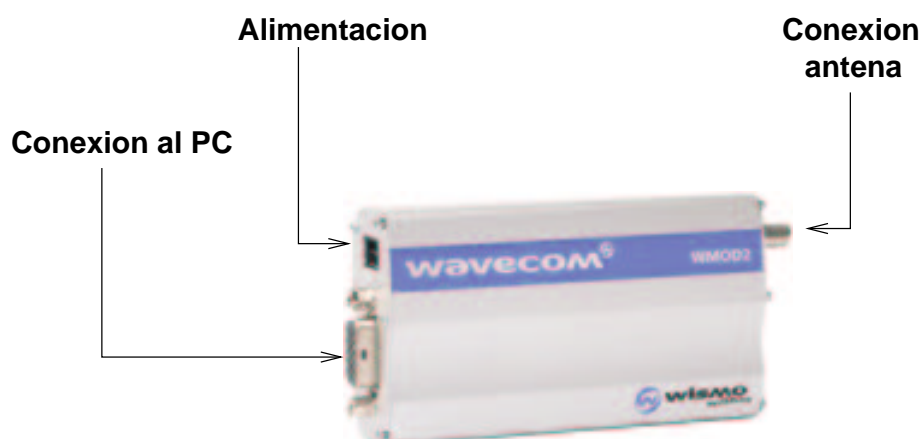


Figura 16: Un módem GSM para PC

TTL (Modems para Circuito impreso).

El estándar “de facto” para controlar los modems se basa en los **comandos AT HAYES**, o más comúnmente conocidos como **comandos AT**. El módem, antes de realizar una conexión con otro módem, se encuentra en *modo comando*. En este modo podemos configurar y controlar el módem utilizando los **comandos AT**. Una vez establecida la conexión con un módem remoto, se pasa del modo comando al *modo conexión*, por lo que la información que le llega al módem por la línea serial no es interpretada como **comandos AT** sino como información a transmitir. Una vez terminada la conexión el módem vuelve al *modo comando*.

Los **comandos AT** con cadenas ASCII que comienzan por los caracteres **AT** y terminan con un *retorno de carro*. 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. En la figura 17 se muestra un ejemplo de comunicación entre un módem y un PC con un terminal de comunicaciones abierto. El usuario teclea el comando “ATZ” seguido de ENTER. El módem interpreta este comando, que es de inicialización y devuelve la cadena “OK” seguida de un retorno de carro para indicar que se ha ejecutado con éxito.

A continuación se listan algunos comandos AT. Se puede encontrar más información en [6, 7]:

- **ATA**: Responder a una llamada entrante
- **ATD**: Llamar a un número de tlf.
- **ATE**: Eco de comandos ON/OFF
- **ATF**: Seleccionar modo de conexión
- **ATH**: Colgar/Descolgar

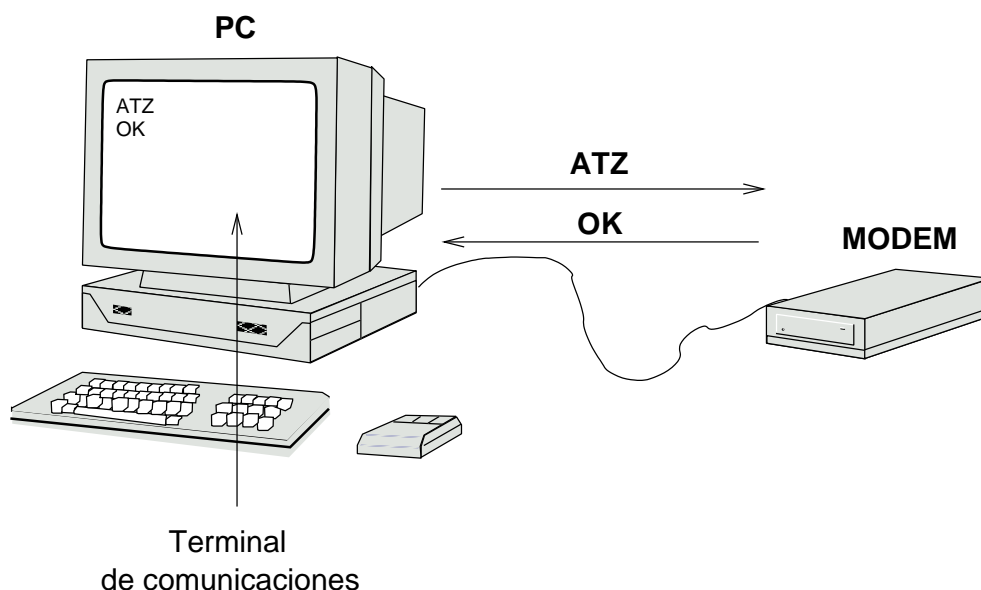


Figura 17: Conexión entre un Módem y un PC

- **ATI:** Obtener identificadores
- **ATL:** Volumen del altavoz
- **ATM:** Control del altavoz
- **ATS:** Lectura/escritura de registros
- **ATZ:** Reset del módem

4.3. Interfaz con Modems GSM

Los modems GSM no sólo se comportan de forma muy parecida a un modem normal, permitiendo el intercambio de datos con otro modem 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 las letras AT+, y se denominan **comandos AT+**.

4.3.1. Comandos AT+

En este apartado se listan algunos de los comandos AT+ implementados en los modems GSM para tener una idea de lo que se puede controlar a través del modem, aunque existen muchos más

comandos[8]

1. **Comandos generales**

- a) **AT+CGMI**: Identificación del fabricante
- b) **AT+CGSN**: Obtener número de serie
- c) **AT+CIMI**: Obtener el IMSI.
- d) **AT+CPAS**: Leer estado del modem

2. **Comandos del servicio de red**

- a) **AT+CSQ**: Obtener calidad de la señal
- b) **AT+COPS**: Selección de un operador
- c) **AT+CREG**: Registrarse en una red
- d) **AT+WOPN**: Leer nombre del operador

3. **Comandos de seguridad:**

- a) **AT+CPIN**: Introducir el PIN
- b) **AT+CPINC**: Obtener el número de reintentos que quedan
- c) **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
 - Modo texto
 - 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 modem GSM conectado al puerto serie y un terminal de comunicaciones. El esquema es el mismo que el mostrado en la figura 17. Si el sistema operativo empleado es Linux, se puede utilizar el programa **minicom** [11]. En el caso de Windows, se puede emplear el **Hyperterminal**.

■ Lectura de la lista de teléfonos

Para listar todos los teléfonos se utiliza el comando AT+CPBR. Primero comprobamos la capacidad del directorio telefónico:

```
AT+CPBR=?  
+CPBR: (1-150),20,14  
OK
```

La información devuelta nos indica que el directorio tiene 150 entradas, desde la 1 hasta la 150, y que en cada entrada el teléfono puede ocupar como máximo 20 caracteres y el texto 14. Para listar los teléfonos debemos indicar qué entradas se quieren examinar. Como en este SIM hay 150 como máximo, utilizamos el siguiente comando:

```
AT+CPBR=1,150  
+CPBR: 1,"607557556",129,"JAIME"  
+CPBR: 2,"915541831",129,"QUINTANAJ"  
+CPBR: 3,"914465076",129,"PACO PIO"  
+CPBR: 4,"914634436",129,"MARIANO"  
+CPBR: 5,"915338584",129,"ANGEL"  
+CPBR: 6,"617203473",129,"MOVIL TOR"  
+CPBR: 7,"679453250",129,"Virginia"  
+CPBR: 8,"629040222",129,"Paloma M"  
  
OK
```

Se listan todos los teléfonos comprendidos entre las entradas 1 y 150. En total hay 8, que ocupan las posiciones 1-8. Para listar las 3 primeras entradas habría que hacer lo siguiente:

```
AT+CPBR=1,3  
+CPBR: 1,"607557556",129,"JAIME"  
+CPBR: 2,"915541831",129,"QUINTANAJ"  
+CPBR: 3,"914465076",129,"PACO PIO"  
  
OK
```

Para una entrada sólo hay que especificar su número:

```
AT+CPBR=7
+CPBR: 7,"679453250",129,"Virginia"
```

```
OK
```

■ 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 <categoria> 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: 2,"REC READ","609","02/02/27,18:16:51+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: 3,"REC READ","1122","02/02/28,20:41:25+40"
-
Bienvenido a Omitel Vodafone! Para acceder a su buzón de voz marque
123,servicio de Atención al Cliente marque 609 (llamadas no gratuitas
desde el extranjero)
+CMGL: 4,"REC READ","+34609100609","02/05/06,10:00:16+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
```

Hay tres mensajes recibidos y que han sido leídos.

■ Lectura de un mensaje

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

```
AT+CMGR=2
+CMGR: "REC READ","609","02/02/27,18:16:51+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=1  
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 modem el que se encarga de generar la trama SMS-SUBMIT correspondiente y enviarla. Este es el modo por defecto y el que normalmente se emplea si sólo queremos transmitir un mensaje.

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 modem 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",14
```

que indica que se ha recibido un mensaje SMS y se ha almacenado con el número 14. Si ahora leemos el mensaje:

```
AT+CMGR=14
```

```
+CMGR: "REC UNREAD", "+34630672901", "02/06/23,11:57:20+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 modem 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 modem toma el que tenga predefinido.

5. Construcción de una aplicación de acceso a los servicios SMS

5.1. Introducción

Hasta ahora se ha visto cómo podemos acceder a los **servicios SMS**, así como a mucha más información, utilizando un **modem GSM**, un terminal de comunicaciones y los **comandos AT+**. En este apartado se muestra una aplicación, **GTERM**, que permite realizar las siguientes funciones, directamente desde la barra de aplicaciones:

1. Listar los teléfonos
2. Listar todos los mensajes SMS almacenados
3. Borrar un mensaje
4. Leer un mensaje
5. Enviar un mensaje

Todos la información devuelta por el modem se presenta en pantalla, sin realizar ningún tipo de procesamiento. También se pueden enviar otros comandos AT+, tecleándolos directamente en la zona de entrada de comandos.

Es un programa muy simple, que muestra cómo se pueden hacer aplicaciones más complejas que accedan a todos los servicios proporcionados por GSM.

5.2. Plataforma

5.2.1. Plataforma hardware

Es necesario disponer de un ordenador PC con un puerto serie, un cable serie y un modem GSM. Para la realización de este trabajo, se ha utilizado la tarjeta Dácer (Figura 15), desarrollada en el departamento de I+D de la empresa **Pulsar Technologies**[9], y del que formó parte el autor de este trabajo. Esta tarjeta dispone de un **Modem GSM Wavecom**[10] y de un sistema uCSIMM, basado en el microcontrolador 68EZ328 (Dragonball) de Motorola, y que corre el

sistema operativos **microlinux**[12]. Está pensada para realizar aplicaciones autónomas del PC, pudiéndose conectar a una red Ethernet.

Sin embargo, la aplicación desarrollada en el PC, **Gterm**, se basa en la conexión de un modem GSM para PC. La **tarjeta Dácer** dispone de un modo de configuración en el que todas las salidas del modem se conectan directamente a un conector DB9 hembra, lo que permite acceder al módem desde un PC cualquier. Así que a todos los efectos, la **tarjeta Dácer** se está empleando exclusivamente como un **módem GSM** para PC¹ y en todas las figuras y explicaciones se tratará como tal, no haciéndose más referencia a **Dácer**.

El módem GSM empleado es un WAVECOM WMOi3 para circuito impreso[13], no obstante, se puede emplear un WAVECOM FASTRACK con conexión directa a un PC[14].

5.2.2. Plataforma Software

Como sistema de desarrollo software se ha utilizado una plataforma Linux con la siguientes características:

- **Distribución:** Debian Woody (3.0)[15]
- **Versión del Kernel:** 2.4.18[16]
- **Entorno:** Gnome-1.4[17]
- **Librerías gráficas:** GTK+ 1.2[18]
- **Compilador de C:** GCC, 2.95.4[19]
- **Entono de desarrollo gráfico:** Glade, 0.6.4[20]

5.3. Descripción de la aplicación

La aplicación **Gterm** está constituida por tres módulos, como se muestra en la figura 18: *serie.c*, *gterm.c* e *interface.c*.

El módulo *interface.c* es el que construye la interfaz de usuario a partir de un fichero XML generado con la aplicación **Glade**. Además se conectan las señales con las funciones de retrollamada² asociadas al interfaz (pulsación de botón, apertura de menús, introducción de un comando nuevo...).

El acceso al modem se realiza a través del módulo *serie*, que permite abrir el puerto serie, configurarlo adecuadamente (9600 baudios, 8 bits de datos, 1 de stop y sin paridad), realizar lecturas/escrituras y cerrarlos.

El módulo principal, *gterm.c*, recibe las señales provenientes del interfaz y envía los comandos AT al modem, además de mostrar en pantalla todo lo que se recibe del modem.

¹El autor de este trabajo no dispone de un modem GSM para conectar directamente al PC, pero sí dispone de una tarjeta Dácer, puesto que participó en su diseño. Por ello este trabajo se ha realizado con dicha tarjeta, pero se puede sustituir por un modem GSM para PC, y el software funcionará exactamente igual.

²Se ha traducido callback function por función de retrollamada

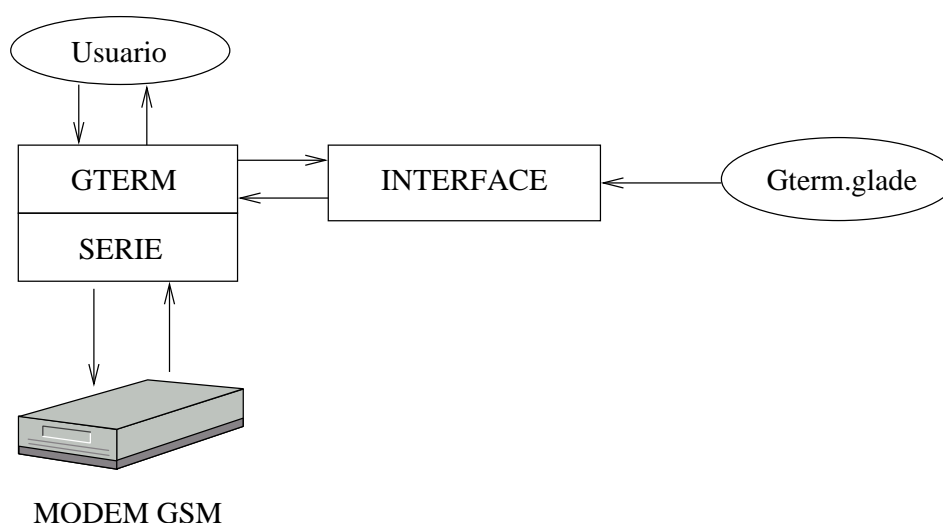


Figura 18: Diagrama de bloques de gterm

Por tratarse de una aplicación muy sencilla para mostrar el funcionamiento de los modems GSM, se le ha dotado de la funcionalidad mínima. La conexión del modem sólo se puede realizar a través del dispositivo `/dev/ttyS0` (COM1). Para realizarla a través de otro puerto hay que modificarlo en el código y recompilar.

El aspecto de la aplicación se muestra en la figura 19. Está dividida en tres zonas:

1. La barra de herramientas, constituida por 7 botones y cuya funcionalidad se muestra en la figura 20
2. La zona de entrada de comandos
3. El terminal que muestra toda la información recibida del modem

5.4. Utilización de Gterm

5.4.1. Conexión inicial

Lo primero que hay que hacer es conectar el modem gsm al ordenador, a través del puerto COM1 (`/dev/ttyS0`). En de utilizar la **tarjeta Dácer** los switches 1 y 2 deben estar en posición **ON**, mientras que el resto en posición **OFF**.

Introducir la tarjeta SIM y alimentar el modem. Ejecutar **gterm** e introducir los comandos **ATZ** y **ATI** para comprobar que la comunicación con el modem es la correcta. En la ventana del terminal debe aparecer lo siguiente:

```
atz
OK
ati
```

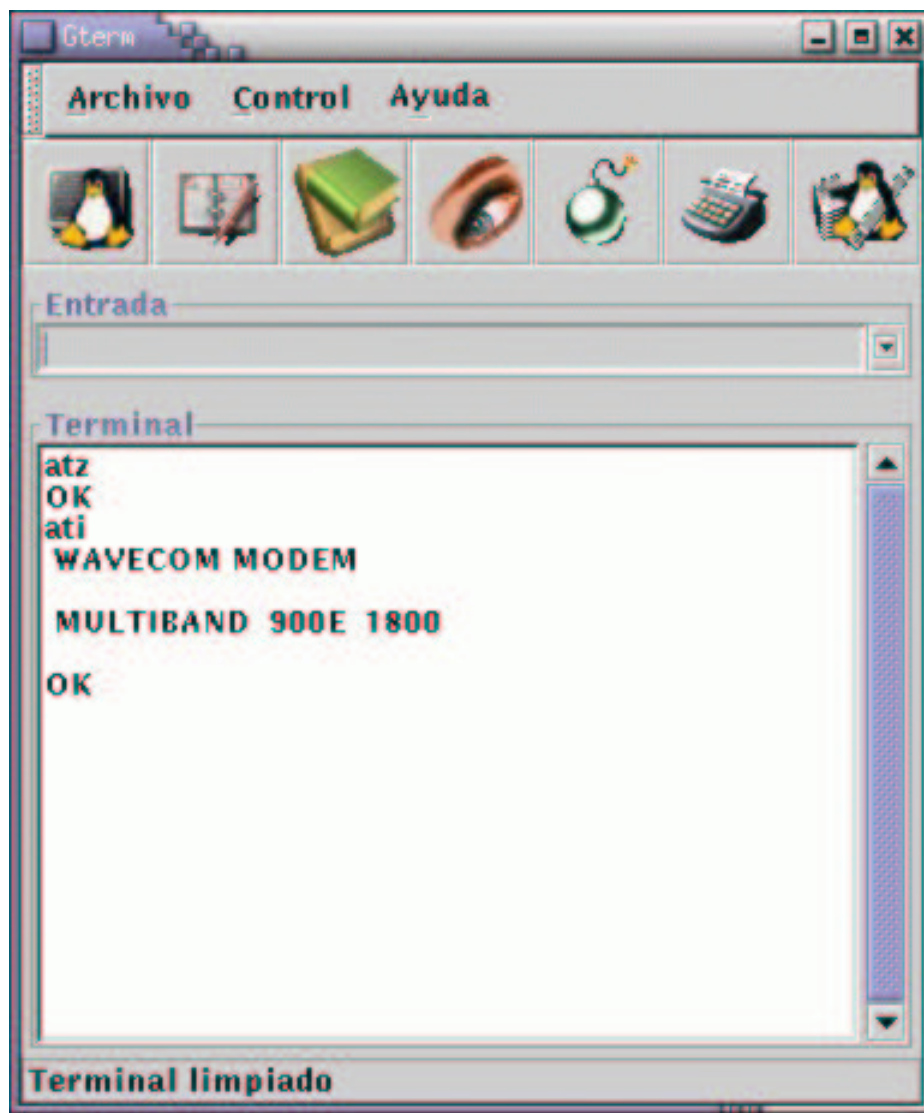


Figura 19: La aplicación gterm

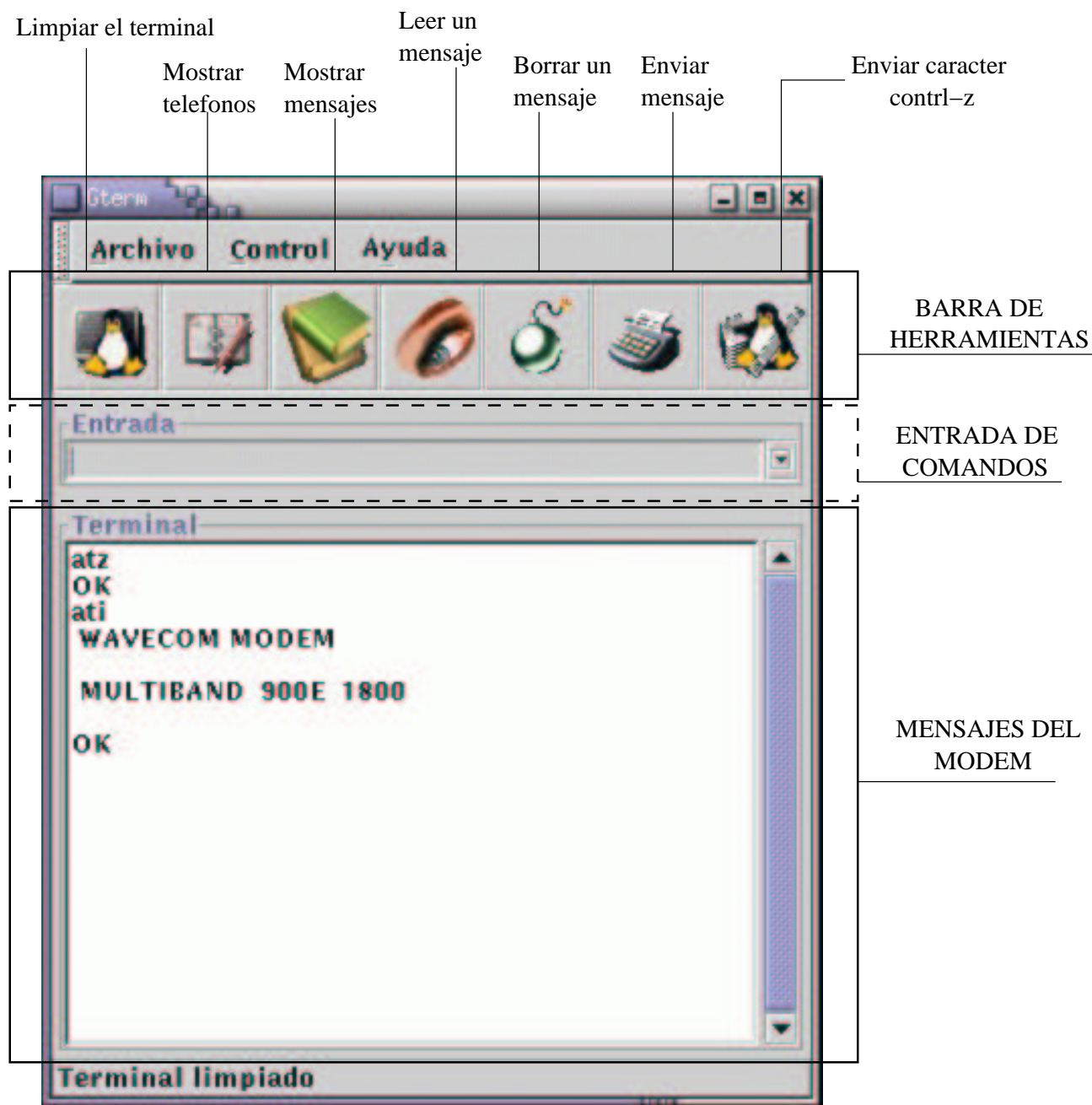


Figura 20: Partes que componen el interfaz de Gterm

```
WAVECOM MODEM  
MULTIBAND 900E 1800  
OK
```

Para poner enviar mensajes y tener acceso a toda la funcionalidad GSM hay que introducir el PIN. Para ello tecleamos el comando AT+CPIN=<pin>:

```
AT+CPIN=7855  
OK
```

Si el pin es incorrecto el modem devolverá el mensaje “ERROR”. En la figura 21 se muestra un ejemplo del proceso de inicialización.

5.4.2. Listando teléfonos y mensajes

Para listar los teléfonos y la lista de mensajes SMS almacenados sólo hay que pulsar los botones correspondientes (o acceder a las opciones desde el menu control). Se envían automáticamente los comandos AT correspondientes y se muestra en el terminal la información volcada por el modem

5.4.3. Lectura y borrado de un sms

Pulsando los botones correspondientes aparecerá un cuadro de diálogo en donde se indica el número de mensaje a visualizar/borrar (Figura 22).

5.4.4. Envío de un mensaje

Sólo hay que pulsar el botón correspondiente de la barra de herramientas e introducir en la caja de diálogo que aparece (figura 23) el teléfono y el mensaje a enviar.

5.5. Listado de la aplicación

5.5.1. Módulo serie.c

Ver fichero serie.pdf

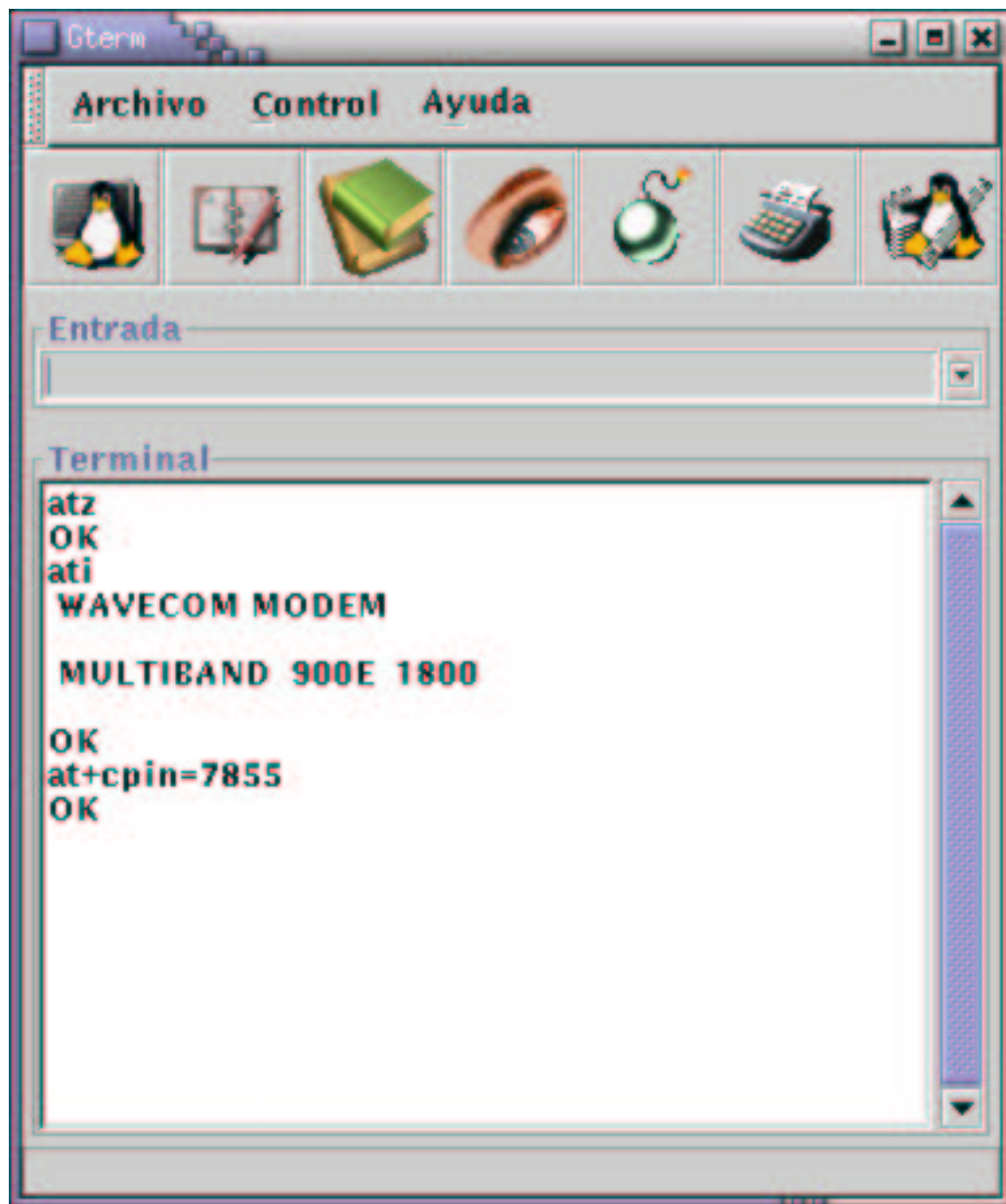


Figura 21: Ejecución inicial de Gterm

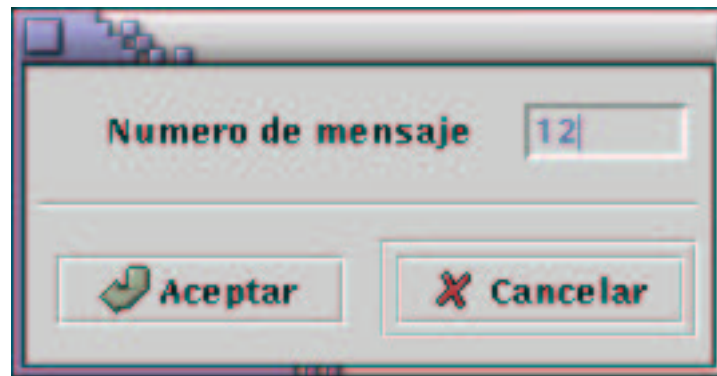


Figura 22: Lectura/borrado de mensajes

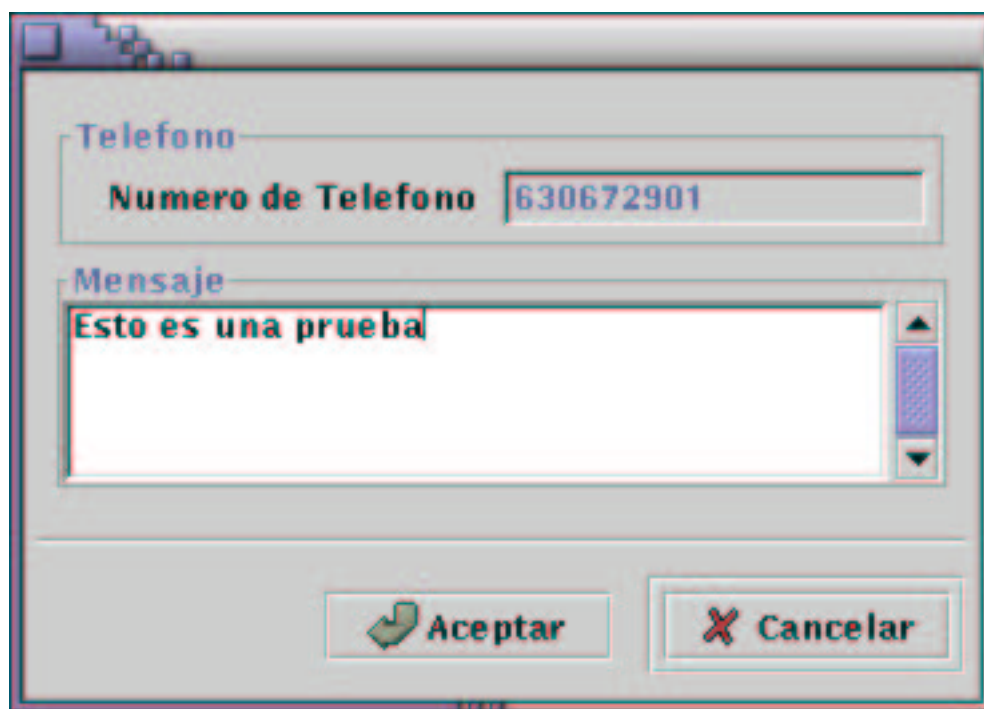


Figura 23: Envío de un SMS

5.5.2. Módulo interface.c

Ver fichero interface.pdf

5.5.3. Programa principal: gterm.c

Ver fichero gterm.pdf

6. Conclusiones

Las conclusiones que se pueden extraer de este trabajo son las siguientes:

- **El sistema GSM es complejo**, sin embargo los modems GSM nos permite hacer abstracción de la red GSM y utilizar sus servicios desde nuestras aplicaciones.
- La forma de controlar los Modems y de acceder a todos los servicios es mediante los **comandos AT**, y **AT+**
- El acceso físico al módem es mediante una **línea serie**, con niveles RS232 (modem gsm para PC) o con niveles TTL
- Para realizar aplicaciones en el PC que accedan a los servicios de GSM y en concreto al servicio de envío/recepción de SMS hay que tener información sobre:
 - **Acceso al puerto serie desde el PC**. Esto depende del sistema operativo empleado
 - Descripción y sintáxis de los **comandos AT** y **AT+**
- La complejidad de la aplicación no depende en sí de los servicios GSM que usa sino de la funcionalidad que se le quiera dar. Los mecanismos de acceso al modem para enviar/recibir SMS son sencillos.

7. Líneas futuras

Posibles líneas de ampliación para este trabajo, en un futuro son las siguientes:

- A nivel teórico, un estudio de SMS sobre GPRS para responder a las siguientes preguntas:
 - ¿El protocolo SM-TL es el mismo?
 - En caso negativo, ¿Cuál es el nuevo protocolo?
 - ¿Usan los modems GPRS el mismo interfaz basado en comandos AT+?
- A nivel práctico son muchas las aplicaciones que se pueden desarrollar, tomando de base la aplicación Gterm, desarrollada en este trabajo:
 - Servidor de envío de SMS para un intranet. Hacer un programa servidor que permite que ciertos clientes se conecten a él y puedan enviar mensajes SMS
 - Servidor de SMS, que procese los mensajes SMS entrantes y que responda devolviendo los datos solicitados o que realice las acciones indicadas en el SMS. Ej. comprobar remotamente el estado de un servidor, para saber si está o no caído.
 - Conexión de un modem GSM a un sistema microcontrolador para hacer aplicaciones autónomas que permitan:
 - Telemetría
 - Telecontrol
 - Envío de Alertas
 - ...

8. Glosario de términos

- **MS:** Mobile Station
- **BS:** Base Station
- **BTS:** Base Transceiver Station
- **BSC:** Base Station Controller
- **BSS:** Base Station Subsystem
- **RSS:** Radio SubSystem
- **MSC:** Mobile Switching Center
- **GMSC:** Gateway Mobile Service Switching Center
- **HLR:** Home Location Register
- **VLR:** Visitor Location Register
- **SME:** Short Message Entity
- **SC:** Service Center
- **PLMN:** Public Land Mobile Network
- **SMS-GMSC:** Gateway MSC For Short Message Service
- **SMS-IWMSC:** Interworking MSC For Short Message Service
- **IMSI:** International Mobile Subscriber Identity

Referencias

- [1] Etsi. European Telecommunications Standards Institute. www.etsi.org
- [2] “Comunicaciones móviles”. Francisco Gómez. Documentación de la Asignatura de doctorado “Nuevas tecnologías para las comunicaciones”. Curso 2001/02
- [3] “Trasmisión por Radio”. José María Hernando Rábanos. Ed. Centro de estudios ramón areces, S.A. Segunda edición.
- [4] “Technical realization of the Short Message Service (SMS) Point-to-Point”. GSM-03.40. Version 5.3.0. ETSI.
- [5] Búsqueda en google: “AT hayes commands”.

- [6] Descripción de los comandos AT de Hayes. <http://www.cellular.co.za/hayesat.htm>.
- [7] Otra referencias de comandos AT. <http://www.modemhelp.net/basicatcommand.shtml>
- [8] “AT commands interface”. WAVECOM. Version 8.4.
http://www.icenet.cz/pdf/WM_SW_OAT_IFS_001_001.pdf.
- [9] Empresa Pulsar Technologies. www.pulsartec.com.
- [10] Empresa WaveCom, fabricante de modems GSM entre otras cosas. www.wavecom.com.
- [11] Programa Minicom. Terminal de comunicaciones para Linux.
<http://www.netsonic.fi/~walker/minicom.html>
- [12] Sistema operativo microlinux (uClinux). <http://www.uclinux.org/>
- [13] Modem GSM para CI de Wavecom. http://www.wavecom.com/products/integra_modem.php
- [14] Modem GSM para PC de Wavecom. http://www.wavecom.com/products/fastrack_modem.php
- [15] Página oficial de Debian. <http://www.debian.org>
- [16] Kernels de Linux. <http://www.kernel.org/>
- [17] Escritorio Gnome. <http://www.gnome.org>
- [18] Librerías gráficas GTK+ multiplataforma para diseño de interfaces gráficos.
<http://www.gtk.org>
- [19] Compilador de C de GNU. <http://gcc.gnu.org/>
- [20] Aplicación para desarrollo de interfaces gráficos con GTK+. <http://glade.gnome.org/>