

短信 PDU 编码解码

有两种方式，一有短信网关，二是通过 SMS 的 DTE-DCE 接口标准(AT 命令集)。我们来讨论一下 At 命令发送短信，下面是在 Siemens M75 验证。

一共有三种方式来发送和接收 SMS 信息：Block Mode, Text Mode 和 PDU Mode。其中 PDU Mode 被所有手机支持，可以使用任何字符集，这也是手机默认的编码方式。其中又分 7bit-160, 8bit-140, 16bit-70 的方式，我们中文用 16bit70 的方式。

在 Text Mode 下，发送及接收到的数据均以 ASCII 码的形式来表示。在 PDU Mode 下，短信息正文经过十六进制编码后被传送。PDU 相当于一个数据包，它由构成消息（SMS）的信息组成。作为一种数据单元，它必须包含源/目的地址、保护（有效）时间、数据格式、协议类型和正文，正文长度可达 140 字节，它们都以十六进制表示。PDU 结构根据短消息由移动终端发起或以移动终端为目的而不同。每条消息可以发送 140 个字节，由于本系统中最长的数据串没有超过 140 个字节，因此数据均可以用一条消息来发送。

现举例说明短消息的发送与接收（以 Text Mode 为例）

（1）设置短消息中心

AT+CSCA="+8613800100500" (短消息中心号码)

（2）设置短消息发送格式

AT+CMGF=1 (1-TEXT; 0-PDU)

（3）发送短消息(短消息内容为"ABCD")

AT+CMGS="13694121067" (目的地址)

> ABCD ^z

（4）设置新短消息到达提示

AT+CNMI=1,1,0,0,1()

当短消息到达时，模块将自动发出提示指令： +CMTI:"SM",INDEX(信息存储位置)

（5）读取短消息内容，假设 INDEX=8。

AT+CMGR=8

返回信息如下：

+CMGR: "REC READ","+8613694121067","04/05/31,11:21:18+00"

HELLO

（6）删除短消息

AT+CMGD=INDEX

考虑到 GSM 传输存在时延问题，与卫星传输方式一样，双方的数据收发均只采用自报方式。即：终端站采用定时自报方式主动向后台中心发射数据，后台中心被动接收；当后台中心需要终端站当前的数据或需要对终端站参数进行设置时，后台中心只向该终端站发射相应的命令包，终端站收到该命令时，根据不同的命令以自报方式发送后台中心所要数据或修改相应的参数。

下面讨论 PDU 方式的编码方式：

例 1 发送：SMSC 号码是+8613800250500，对方号码是 13851872468，消息内容是“Hello! ”。从手机发出的 PDU 串可以是

08 91 68 31 08 20 05 05 F0 11 00 0D 91 68 31 58 81 27 64 F8 00 00 00 06 C8 32
9B FD 0E 01

对照规范，具体分析：

08

SMSC 地址信息的长度

共 8 个八位字节(包括 91)

91

SMSC 地址格式(TON/NPI)

用国际格式号码(在前面加‘+’)

68 31 08 20 05 05 F0

SMSC 地址

8613800250500，补‘F’凑成偶数个

11

基本参数(TP-MTI/VFP)

发送，TP-VP 用相对格式

00

消息基准值(TP-MR)

0

0D

目标地址数字个数

共 13 个十进制数(不包括 91 和`F`)

91

目标地址格式(TON/NPI)

用国际格式号码(在前面加`+`)

68 31 58 81 27 64 F8

目标地址(TP-DA)

8613851872468, 补`F`凑成偶数个,BCD 编码方式, 低位-高位方式

00

协议标识(TP-PID)

是普通 GSM 类型, 点到点方式

00

用户信息编码方式(TP-DCS)

7-bit 编码

00

有效期(TP-VP)

5 分钟

06

用户信息长度(TP-UDL)

实际长度 6 个字节

C8 32 9B FD 0E 01

用户信息(TP-UD)

"Hello!"

0891683108100005F0 31 00 0B 81 3129503323F1 00 08 A8 0C
4F6060F3776189C94E865427

分析一下

分段

含义

说明

08

SMSC 地址信息的长度

共 8 个八位字节(包括 91)

91

SMSC 地址格式(TON/NPI)

用国际格式号码(在前面加'+'), 81 表示没有+

683108100005F0

SMSC 地址

8613800100500, 补'F'凑成偶数个 bcd 编码

31

基本参数(TP-MTI/VFP)

发送, TP-VP 用相对格式。标志

00

消息基准值(TP-MR)

0

0D

目标地址数字个数

共 13 个十进制数(不包括 91 和'F')

81

目标地址格式(TON/NPI)

用国际格式号码(在前面加'+'), 81 表示没有'+'

3129503323F1

目标地址(TP-DA)

8613851872468, 补'F'凑成偶数个,BCD 编码方式, 低位-高位方式

00

协议标识(TP-PID)

是普通 GSM 类型, 点到点方式

08

用户信息编码方式(TP-DCS)

16-bit 编码, UCS2 编码

A8

有效期(TP-VP)

2 天

0C

用户信息长度(TP-UDL)

实际长度 12 个字节

4F6060F3776189C94E865427

用户信息(TP-UD)

"你睡觉了吧!"

在 PDU Mode 中, 可以采用三种编码方式来对发送的内容进行编码, 它们是 7-bit、8-bit 和 UCS2 (16bit) 编码。7-bit 编码用于发送普通的 ASCII 字符, 它将一串 7-bit 的字符(最高位为 0)编码成 8-bit 的数据, 每 8 个字符可"压缩"成 7 个; 8-bit 编码通常用于发送数据消息, 比如图片和铃声等; 而 UCS2 编码用于发送 Unicode 字符。在这三种编码方式下, PDU 串的用户信息(TP-UD)段最大容量(可以发送的短消息的最大字符数)分别是 160、140 和 70。

这里，将一个英文字母、一个汉字和一个数据字节都视为一个字符。

Unicode 字符编码解码如下

```
// UCS2 编码

// 输入: pSrc - 源字符串指针

//      nSrcLength - 源字符串长度

// 输出: pDst - 目标编码串指针

// 返回: 目标编码串长度

int gsmEncodeUcs2(const char* pSrc, unsigned char* pDst, int nSrcLength)
{
    int nDstLength;          // UNICODE 宽字符数目

    WCHAR wchar[128]; // UNICODE 串缓冲区

    // 字符串-->UNICODE 串

    nDstLength = MultiByteToWideChar(CP_ACP, 0, pSrc, nSrcLength, wchar,
128);

    // 高低字节对调，输出

    for(int i=0; i<nDstLength; i++)
    {
        *pDst++ = wchar[i] >> 8;          // 先输出高位字节

        *pDst++ = wchar[i] & 0xff;        // 后输出低位字节
    }

    // 返回目标编码串长度
```

```

        return nDstLength * 2;
    }

// UCS2 解码

// 输入: pSrc - 源编码串指针

//      nSrcLength - 源编码串长度

// 输出: pDst - 目标字符串指针

// 返回: 目标字符串长度

int gsmDecodeUcs2(const unsigned char* pSrc, char* pDst, int nSrcLength)
{
    int nDstLength;      // UNICODE 宽字符数目

    WCHAR wchar[128]; // UNICODE 串缓冲区

    // 高低字节对调, 拼成 UNICODE

    for(int i=0; i<nSrcLength/2; i++)
    {
        wchar[i] = *pSrc++ << 8;  // 先高位字节

        wchar[i] |= *pSrc++;      // 后低位字节
    }

    // UNICODE 串-->字符串

    nDstLength = WideCharToMultiByte(CP_ACP, 0, wchar, nSrcLength/2, pDst,
160, NULL, NULL);

```

```
// 输出字符串加个结束符

pDst[nDstLength] = '\0';


// 返回目标字符串长度

return nDstLength;

}
```