PIML900/1800 GPRS 使用说明

北京康泰新锐科技发展有限公司

技术支持：毕庆贞

2004.08.09

本文描述了用 PIML900/1800 模块实现数据传输的协议过程。当利用模块实现据传输时，模块通过 PPP 协议与 CMNET 网关进行通信，然后由 CMNET 网关连接到 Internet。

一． 协议流程图

拨通 GPRS 后，用 LCP、IPCP 和 CMNET 握手，用 IP 和 TCP/UDP 是实现数据传输。下面是几种协议的具体实现过程。

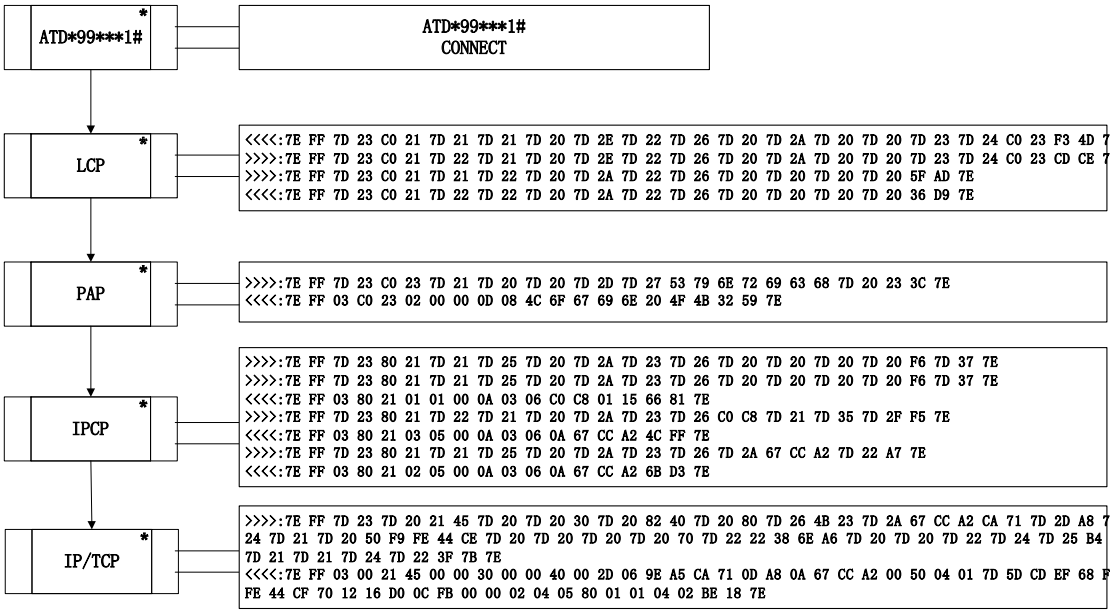

图 1 PPP 协议流程图

二．协议解析

1． 拨通 GPRS

对于 PIML900/1800 模块，在中国现有的网络中，可以通过下列的命令拨通 GPRS 网络：

AT+CGATT=1 //激活 GPRS 服务

OK

AT+CGDCONT=1,”IP”,”cmnet” //定义一个 PPP 连接

OK

ATD*99***1# //拨号

CONNECT

7EFF7D23C0217D217D217D207D2E7D227D267D207D2A7D207D207D237D24C023F34D7E

2． PPP 协议解析

2.1 PPP 协议的数据包格式

表 1　PPP 数据包格式

Start Flag	Address	Control	Protocol	Code	ID	Length	Info	Checksum	End Flag
0x7E	0xFF	0x03	(2 Bytes)	(1 Byte)	(1 Byte)	(2 Bytes)	(Variable)	(2 Bytes)	0x7E

2.2 PPP 数据包的解析

（1）标志位（Flag）：指示一个 PPP 包的开始或结束，它的起始位和结束位都是 0x7E，可以根据数据包是由 7E 开始和 7E 结束来判断这个数据包是 PPP 数据包。

（2）地址域（Address）：FF，是一个标准的广播地址，PPP 并不指定单个工作站的地址。

（3）控制域（Control）：03，这个表示用户采取无序帧方式传输。

（4）协议域（Protocol）：用于标识封装在 PPP 数据包信息域中的协议类型。

表 2　协议说明

Protocol	Description
0xC021	Link control protocol (LCP)
0xC023	Password authentication protocol (PAP)
0x8021	Internet protocol control protocol (IPCP)
0x0021	Internet protocol

（5）命令代码（Code）

表3 命令代码说明

Type	Packet Type	Description
0	Vendor specific	Proprietary vendor extensions
1	Configure-request	Configuration options the sender desires to negotiate
2	Configure-ack	Configuration options the sender is acknowledging
3	Configure-nak	Unacceptable configuration options from the configure-request packet; acceptable values are included
4	Configure-reject	Configuration options are not recognizable or are not acceptable for negotiations
5	Terminate-request	Terminate this link
6	Terminate-ack	Terminate acknowledge
7	Code-reject	Reception of an LCP packet with an unknown code
8	Protocol-reject	Reception of a PPP packet with an unknown protocol field
9	Echo-request	Initiation of a loopback mechanism
10	Echo-reply	Response to an echo-request
11	Discard-request	Discard this packet for testing and debugging purposes

（6）命令的标识序列号（ID）

（7）数据长度（Length）

包含协议域、命令代码、标识序列号、长度域和数据域的长度，按照字节计算。

（8）数据域（Information）：长度为 0 或者是多个字节。

（9）检测序列（FCS）：通常为 2 个字节，以检测 PPP 数据包的合法性。

3. LCP 协议解析

LCP 协议是第一个握手协议，具体内容请参考[RFC1661]。在本文中，把 PPP 协议进行了合理的简化，删除了一些在实际应用中没有多少实用价值的部分，这样以便于更快速地建立和拆除链接。

3.1 CMNET->Terminal Config-Req

7EFF7D23C0217D217D217D207D2E7D227D267D207D2A7D207D207D237D24C023F34D7E

按照协议要求，去掉“7D”得：

7EFF03C0210101000E0206000A00000304C023F34D7E

数据内容的具体含义如下：

7E PPP 起始符（Flag）

FF 广播地址（Address）

03 控制位（Control）

C021 协议域（Protocol），C021 代表 LCP

01 命令代码（Code），建链请求（Req）

01 标识符（Identifier）

000E 数据长度

建链请求的数据域：

02 异步控制字符映射

06 Length（0206000A0000）

000A0000

03 认证协议

04 Length（0304C023）

C023 CHAP 认证协议

F34D FCS

7E PPP 结束符（Flag）

3.2 Terminal->CMNET Config-Ack

7EFF7D23C0217D227D217D207D2E7D227D267D207D2A7D207D207D237D24C023CDCE7E

按照协议要求，去掉“7D”得：

7EFF03C0210201000E0206000A00000304C023CDCE

同意建链请求的选项。

3.3 Terminal->CMNET Config-Req

7EFF7D23C0217D217D227D207D2A7D227D267D207D207D207D205FAD7E

按照协议要求，去掉“7D”得：

7EFF03C0210102000A0206000000005FAD7E

向 CMNET 的建链请求。

3.4 CMNET->Terminal Config-Ack

7EFF7D23C0217D227D227D207D2A7D227D267D207D207D207D2036D97E

按照协议要求，去掉“7D”得：

7EFF03C0210202000A02060000000036D97E

4. PAP 协议解析

PAP 是密码验证协议，它的握手过程要与 LCP 协议协商过的一致，具体内容请参考[RFC1334]

4.1 Terminal->CMNET　　Config-Req

7EFF03C0230100000D0753796E7269636800233C7E

4.2 CMNET->Terminal　　Config-Ack

7EFF03C0230200000D084C6F67696E204F4B32597E

5. IPCP 协议解析

IPCP 协议是一个从 CMNET 获得 IP 地址的过程，具体内容请参考[RFC1332]

5.1 Terminal->CMNET　　Config-Req

7EFF0380210105000A030600000000F67D377E

请求一个 IP 地址

5.2 CMNET->Terminal　　Config-Req

7EFF0380210101000A0306C0C8011566817E

请求确认一个服务器地址

5.3 Terminal->CMNET　　Config-Ack

7EFF0380210201000A0306C0C8017D350FF57E

确认了一个服务器地址“C0C8017D”

5.4 CMNET->Terminal　　Config-Nak

7EFF0380210305000A03060A67CCA24CFF7E

提供了一个可用的 IP 地址

5.5 Terminal->CMNET　　Config-Req

7EFF0380210105000A03060A67CCA202A77E

5.6 CMNET->Terminal　　Config-Ack

7EFF0380210205000A03060A67CCA26BD37E

得到一个 IP 地址“0A67CCA2”

6. TCP/IP 协议解析

6.1 TCP/IP 协议的数据包格式

IPV4 的数据包格式如下图，具体的含义见[RFC791]。

<table>
<tr><td>Version</td><td>IHL</td><td>TOS</td><td colspan="2">Total Length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td>Fragment Offset</td></tr>
<tr><td>TTL</td><td colspan="2">Protocol</td><td colspan="2">Header Checksum</td></tr>
<tr><td colspan="5">Source IP Address</td></tr>
<tr><td colspan="5">Destination IP Address</td></tr>
<tr><td colspan="5">Options and Padding</td></tr>
</table>

图 2 IP 数据包格式

IPV4 的数据包格式如下图，具体的含义见[RFC793]。

Source Port			Destination Port
Sequence Number			
Ack Sequence Number			
HeadLength	Reserved	Code	Window Size
Checksum			Urgent Point
Options			Padding
DATA….			

图 3 TCP 数据包格式

6.2 Terminal->CMNET->Internet Server Config-Req

7EFF03002145000030008240008006 4B230A67CCA2CA710DA804010050F9FE44CE00000000700222386EA60000020405B4010104023F7B7E

具体含义如下：

7E PPP 起始符（Flag）

FF 广播地址（Address）

03 控制位（Control）

0021 协议域（Protocol），0021 代表 IP 包

//IP 数据包的内容

4 版本号（Version），4 代表 IPV4

5 IP 头部长度（IHL），以 32 位为一个计算单位

00 服务种类（Type Of Service）

0030 IP 包的长度（Total Length）,以字节为计算单位

0082 IP 包的序号（Identification）

4000 不允许 IP 包分片

80 存活时间（TTL）

06 协议（Protocol）,06 代表了 TCP 协议

4B23 IP 头部校验和（Header Checksum）

0A67CCA2 源 IP 地址（Source IP Address），Cmnet 给我们提供的 IP 地址

CA710DA8 目标 IP 地址（Destination IP Address）

//TCP 数据包的内容

0401 源端口（Source Port）

0050 目标端口（Destination Port）

F9FE44CE 初始序列号（Sequence Number）

00000000 确认序列号（Ack Sequence Number）

7 头部长度（Head Length）

002 保留位和协议段（Reserved and Code）,02 代表 syn=1，即建链初始包的标志

2238 窗口大小（Window Size）

6EA6 TCP 包的校验和（Checksum）

0000 紧急指针（Urgent Point）

//TCP 选项

02	报文段长度最大值选项（MSS）
04	选项长度
0034	指定本机能够接收一个最大的报文长度
0101	选项之间的分隔
0402	选择性确认支持（可以省去这个选项）
3F7B	FCS 结果
7E	结束符

6.3 Internet Server ->CMNET->Terminal Config-Ack

7EFF03002145000030000040002D069EA5CA710DA80A67CCA2005004017D5DCDEF68F9FE44CF701216D00CFB000002040580010104 02BE187E

6.4 Send and Receive Data

TCP 协议握手后，就可以和在普通的 Internet 网上一样的通过 TCP 协议收发数据了。如果用户用的是 UDP 协议，可以略过 6.2 和 6.3，直接向网络上的服务器发送数据。