DTU 设备的管理协议（IHDMP）

使用说明

资料版本：V3.0---20190121

北京映翰通网络技术有限公司

http://www.inhand.com.cn

目录

1. 引言 1
1.1 编写目的 1
1.2 术语定义 1
2. 功能说明 2
2.1 需求说明 2
2.2 下发配置的方式 2
3. 协议内容 3
3.1 数据格式 3
3.2 字节序 3
3.3 数据包格式 3
3.4 DTU 设备的控制部分 3
3.4.1 探测 DTU 3
3.4.2 登录 DTU 4
3.4.3 重启 DTU 4
3.4.4 激活 DTU 连接网络 4
3.4.5 读取 DTU 的特定状态 5
3.4.6 读取 DTU 的当前时间 5
3.4.7 收发短信 6
3.5 DTU 设备的配置部分 9
3.5.1 读取 DTU 的配置 9
3.5.2 读取指定配置 10
3.5.3 设置 DTU 的配置 10
3.5.4 设置单个配置 10
4. 流程描述 11
4.1 探测 11
4.2 读取配置 11
4.3 下发配置 12
5. 附录 13
5.1 附录 1：CRC16 源码 13
5.2 附录 2：配置项的 TAG 描述 15
5.3 附录 3：状态项的 TAG 描述 20

1. 引言

1.1 编写目的

用户设备可以通过串口配置及监控 DTU，以利于设备的调试，检验，装配。

1.2 术语定义

- DTU： 映翰通无线数据终端
- 用户设备：用户接在 DTU 本地串口及本地串口 2 的设备
- 用户数据：用户设备需要通过 DTU 透传的数据
- 配置数据/配置包：符合配置 DTU 配置协议（即本协议）的数据
- 短信命令包/短信命令数据：包含发送短信命令的配置包（详见：发送短信命令）
- 帧：计量串口通信数据的单位。DTU 分帧机制为：串口收到的数据长度大于帧大小或者串口在等待扫描间隔后无数据，则当前数据内容被当做一帧。
- TLV：一种可变长度的数据封装格式
- Hex：16 进制
- IHDMP：映翰通自主开发的 DTU 管理协议

2. 功能说明

2.1 需求说明

读取、配置和监控 DTU 需求：

设备组装好之后，配置 DTU 将变得复杂，所以需要用户设备可直接配置和读取 DTU，以利于生产调试、检验，装配。

用户设备也需要监控 DTU 设备的状态，用来分析和解决故障，统计流量等。甚至部分用户需要在使用 IP 数据流量链路的同时收发短信。

相应需求解决方案:

用户设备与 DTU 的交互，采用同一套协议，所有数据采用 TLV 格式，不同 TAG 代表不同的配置项或者状态项，通过串口可以读写 DTU 的配置，收发短信，读取通讯模组的状态。

通过 DTU 设备的管理协议，简称 IHDMP，可实现：

- 读取/下发 DTU 配置
- 读取 DTU 状态
- 发送/接收短信
- 恢复出厂设置
- 重启 DTU

2.2 下发配置的方式

用户设备可以通过本地串口和本地串口 2 下发配置包。其中，本地串口 1 有 4K 缓存用于缓存用户数据和发短信命令包（关于短信发送功能参考短信发送功能），但是普通配置包只有 1K 缓存；本地串口 2 有 1K 缓存。所以下发配置包与用户数据时：

注意事项：

1. 用户设备不能将用户数据与配置包放在同一帧下发；
2. 下发用户数据与配置包之间、配置包与配置包之间时间间隔必须大于设置的串口扫描间隔（本地串口和本地串口 2 有各自的串口扫描时间，可通过 InHand DTU 配置工具设置，默认为 200ms）；
3. 用户设备下发的配置数据总长度不得大于设置的帧大小（本地串口和本地串口 2 有各自的帧大小，可通过 InHand DTU 配置工具设置，默认为 1024 字节），否则由于分帧导致数据破坏；
4. 如果用户设备下发配置数据不符合本协议，DTU 不会给出应答。

3. 协议内容

本协议规定了用户设备（上位机）与 DTU 交互的通信规范。

3.1 数据格式

本协议所有交互数据都为 16 进制数。

3.2 字节序

本协议数据在传输时采用网络字节序，既大端字节序。

3.3 数据包格式

- 输入给 DTU：

包头	命令字	包体长度	包体	CRC16
55 AA 55 AA	1 字节	2 字节	TLVs	2 字节

- DTU 输出：

包头	命令字	包体长度	包体	CRC16
AA 55 AA 55	1 字节	2 字节	TLVs	2 字节

注意事项：

不同的功能选用不同的命令字，具体请参照 3.4~3.5 章节的描述。

CRC 校验算法请参阅附录 1：CRC16 源码，可以直接调用 byAddCrc16 函数得到 CRC16 值，其中：

DTU 返回的数据包 CRC 校验不包括命令字部分；但下端设备发送给 DTU 时 CRC 需要包括包头，命令字，包体长度及包体部分。

包体长度表示包体的长度，即除去包头、命令字、包体长度及 CRC 之外的数据总长度，有些数据包包体为空则包体长度为 0.

包体采用 TLV 格式，一个配置包可以包括多个 TLVs（TLV 具体定义请参阅附录 2：配置项的 TAG 描述）：

TAG	LENGTH	VALUE
2 字节	2 字节	不定

3.4 DTU 设备的控制部分

3.4.1 探测 DTU

命令字：0x03

用户设备：**55 AA 55 AA 03 00 00 11 65**

DTU：**AA 55 AA 55 03 00 09 81 2A 00 05 30 63 38 30 31 FB F6**

TLVs 部分为：**81 2A 00 05 30 63 38 30 31**

TAG：**81 2A**

LENGTH：**00 05**

VALUE：**30 63 38 30 31** 依次表示登录状态及串口参数。

第一个字节 **30** 表示未登录，**31** 表示管理员身份登录。后四个字节表示串口参数：波特率，数据位，校验方式，停止位。关于串口参数部分定义请参阅附录 2：配置项的 TAG 描述

3.4.2 登录 DTU

命令字：0x05

用户设备：**55 AA 55 AA 05 00 11 81 10 00 03 61 64 6D 81 11 00 06 31 32 33 34 35 36 1F 44**

TLVs 部分为：**81 10 00 03 61 64 6D 81 11 00 06 31 32 33 34 35 36** 包含两个 TLV：

1) 用户名：

TAG：**81 10**

LENGTH：**00 03**

VALUE：**61 64 6D** 是 adm 的 ASCII

2) 密码：

TAG：**81 11**

LENGTH：**00 06**

VALUE：**31 32 33 34 35 36** 是 123456 的 ASCII

DTU：**AA 55 AA 55 05 00 01 01 23 C1** 回应部分只包含 length 为 1 的包体，**01** 表示管理员登录成功。**00** 表示未登录。

3.4.3 重启 DTU

命令字：0x12

用户设备：**55 AA 55 AA 12 00 00 58 BA**

DTU：**AA 55 AA 55 12 00 01 01 23 C1** 回应部分只包含 length 为 1 的包体.

3.4.4 激活 DTU 连接网络

命令字：0x14

激活 GPRS 并连接第一个中心：

用户设备：**55 AA 55 AA 14 00 05 81 85 00 01 01 48 9E**

DTU 回应：**AA 55 AA 55 14 00 00 B8 C9** 回应数据帧为 DTU 收到激活命令的确认；

DTU 无回应收到后即激活并连接。（当前大多数版本已废弃此功能。）

3.4.5 读取 DTU 的特定状态

（部分版本不支持此命令，最新标准版程序支持）

3.4.5.1 例 1：读取设备状态

命令字：0x15

用户设备：**55 AA 55 AA 15 00 04 81 83 00 00 7D 0D** (0x8183 表示设备当前状态)

DTU 回应：**AA 55 AA 55 15 00 05 81 83 00 01 01 0D 9C** (0x01 表示连接主站成功)；具体哪些参数可以用 0x15 命令查询，请参照附录 3：状态项的 TAG 描述。

该 0x15 命令和下文的 0x1A 命令有部分交叉，用户可以自行选用合适的命令。

另外，支持同时读取所有状态：

用户设备发送：**55 AA 55 AA 15 00 00 5D 36**

3.4.5.2 例 2：读取中心掉线次数

1、 读取指定中心的掉线次数,如中心 1

用户设备下发：55 AA 55 AA 15 00 04 83 20 00 00 B8 D4

DTU 回复：AA 55 AA 55 15 00 06 83 20 00 02 00 01 04 9B

其中，TLV：83 20 00 02 00 01 中的 Value 为 0x01，标识与中心断开了一次。

2、 读取全部中心掉线次数

用户设备下发： 55 AA 55 AA 15 00 14 83 20 00 00 83 21 00 00 83 22 00 00 83 23 00 00 83 24 00 00 FF 48

DTU 回复：AA 55 AA 55 15 00 1E 83 20 00 02 00 01 83 21 00 02 00 01 83 22 00 02 00 01 83 23 00 02 00 00 83 24 00 02 00 00 FB 8E

或者：

用户设备发送：**55 AA 55 AA 15 00 00 5D 36**

在 DTU 设备中回复的所有 TLV 组中,提取相应 TLV 即可。

备注：掉线次数统计的是：服务器主动断开连接、服务器重置连接、网络异常断开、运营商主动断开链路等所有与服务器断开的情况。

3.4.6 读取 DTU 的当前时间

（部分版本不支持此命令，最新标准版程序支持）

命令字：0x07

有两种格式，其中 0x00 使用相对时间格式（相对于 1970 年 1 月 1 日），0x01 使用绝对时

间格式（年月日时分秒）。其时间是 DTU 通过 SNTP 协议，从配置的 SNTP 服务器（或者如果没有配置 SNTP 服务器的时候，从默认的 SNTP 服务器）获得的。

3.4.6.1 相对时间格式:

用户设备：**55 AA 55 AA 07 00 01 00 21 9A**

1) 如果时间有效（DTU 得到了校准过的时间），DTU 回应：

AA 55 AA 55 07 00 07 01 54 D3 15 86 01 EF C4 E0

其中 0x01 表示后续 6 字节的时间有效。

54 D3 15 86：从 1970 年 1 月 1 日到当前的 UTC 秒数，注意是用的格林威治时间，北京时间需要加 8*3600 秒；

01 EF：毫秒数，0x1EF=495 表示 0.495 秒；

2) 如果时间无效，DTU 回应：

AA 55 AA 55 07 00 07 00 00 00 00 00 00 00 C5 BC

0x00 表示后续 6 字节的时间无效。(这 6 个字节也会都被填充为 0x00)。

3.4.6.2 绝对时间格式:

用户设备：**55 AA 55 AA 07 00 01 01 A8 8B**

1) 如果时间有效（DTU 得到了校准过的时间），DTU 回应：

AA 55 AA 55 07 00 09 01 0F 02 05 0F 02 32 00 27 1B AF

其中 0x01 表示后续 8 字节的时间有效。

0F 02 05: 年月日，表示(20)15 年 2 月 5 日；

0F 02 32: 时分秒，表示 15 点 2 分 32 秒；

00 27: 毫秒数，0x27=39 表示 0.039 秒；

2) 如果时间无效，DTU 回应：

AA 55 AA 55 07 00 08 00 00 00 00 00 00 00 00 6E 69

0x00 表示后续 8 字节的时间无效。(这 8 个字节也会都被填充为 0x00)。

3.4.7 收发短信

（部分版本不支持此命令，最新标准版程序支持）

3.4.7.1 短信发送功能

◆ 短信发送功能介绍

DTU 支持如下四种短信：

- **定制英文短信**
- **定制中文短信**
- **标准英文短信**
- **标准中文短信**

中文短信每条最多可发送 70 个中文字符，超过 70 则会以长短信发送（分割成多条小于 70 个中文字符的短信，根据长短信协议发送），对于支持长短信的终端设备（目前大多数手机都支持），收到的是一条短信，但是可能会产生多条信息费用；对于不支持长短信的终端，可能收到的是多条信息。用户设备发送中文短信时，需要将中文字符的 UCS2 编码(大端)封装在短信内容 TLV 中。

英文短信每条最多可发送 160 个英文字符，超过 160 个英文字符会以长短信发送（分割成多条小于 160 个英文字符的短信，根据长短信协议发送）。用户设备发送英文短信时，将英文字符的 ASCII 值封装在短信内容 TLV 中下发给 DTU。根据 3GPP 规范《3GPP TS 23.038》，英文短信以 GSM7 bit 编码或者 UCS2 编码传输。为了每条短信能够最大限度承载用户数据以节约通讯成本，DTU 选择以 GSM 7bit 编码发送英文短信，支持发送 ASCII 值介于 0~127 之间的字符。由于 GSM 7bit 编码与 ASCII 编码有差异（例如：@符号的 ASCII 是 0x40，GSM 7bit 编码中为 0x00），ACSII 码值介于 32~126 之间的打印字符中的下列字符显示乱码：

字符	ASCII	GSM 7bit 编码(二进制)
$	0x24	0000010
@	0x40	0000000
[	0x5B	无
\	0x5C	无
]	0x5D	无
^	0x5E	无
_	0x5F	0010001
`	0x60	无
{	0x7B	无
|	0x7C	无
}	0x7D	无
~	0x7E	无

建议发送上述字符时，请使用标准中文短信。普通用户请选用标准英文短信和标准中文短信。

注意事项：

DTU 固件版本 InDTU3XX_STD_V1.4.3 及以后才支持长短信功能

短信发送的注意事项：

1. 章节 2.2 中的注意事项，在这里依然适用；
2. 本地串口 1 可以缓存 4K 的短信命令包，可以以非阻塞的方式发送短信，即：在第一条短

信发送过程中，可以接收第二帧短信命令包，当第一条短信发送成功后发送第二条短信；同时，串口 1 支持同时接收多条短信命令帧，用户设备可以将多条短信命令包组合为一帧（不大于帧大小）发送给 DTU；

3. 本地串口 2 不能缓存短信命令包，以阻塞方式发送短信，即：在第一条短信发送成功之前，不能接受第二帧短信命令包；同时，本地串口 2 不支持同时发送多条短信，如果接收到一帧的短信命令数据中包含多条短信命令，只发送第一条短信；
4. 发送英文短信时，短信内容 TLV 中的 VALUE 填充为短信内容的 ASCII 编码；
5. 发送中文短信时，短信内容 TLV 中的 VALUE 填充为短信内容的大端 UCS2 编码；
6. 短信命令帧中的短信内容长度不能超过 980 字节；

◆ 发送短信命令

命令字：0x13

发送短信格式:

包头	命令字	包体长度	手机号码 TLV	短信格式 TLV	短信内容 TLV	CRC
55 AA 55 AA	13	2 字节	Tag: 81 80 Length: 电话号码长度 Value: 字符串	Tag: 81 81 Length: 2 字节 Value: 当前支持 4 种格式	Tag: 81 82 Length: 短信正文长度 Value: 短信正文	2 字节

发送短信当前支持 4 种短信格式：

- **0 表示定制英文短信**
- **1 表示定制中文短信**
- **2 表示标准英文短信**
- **3 表示标准中文短信**

例如：

发送英文标准短信“1234”到 13912345678.

用户设备：**55 AA 55 AA 13 00 1C 81 80 00 0B 31 33 39 31 32 33 34 35 36 37 38 81 81 00 01 02 81 82 00 04 31 32 33 34 FC DE**

发送中文标准短信“你好”(0x4F 0x60 0x59 0x7D)到 13912345678.

用户设备：**55 AA 55 AA 13 00 1C 81 80 00 0B 31 33 39 31 32 33 34 35 36 37 38 81 81 00 01 03 81 82 00 04 4F 60 59 7D BD 16**

DTU 收到短信命令包后，如果短信命令包正确（包头、命令字、数据格式及 CRC 都正确），DTU 立刻回复确认命令：

命令字：0x17

DTU 的确认命令：**AA 55 AA 55 17 00 05 81 89 00 01 02 38 72** 包体的内容为 1 个字节，0x02 表示收到正确短信数据；如果短信命令包不正确，DTU 无返回。

GPRS 成功发送短信之后，向用户设备发送短信发送回应包：

命令字：0x17

DTU 短信发送回应包：**AA 55 AA 55 17 00 06 81 89 00 01 00 7B 39** 包体的内容为 1 个字节，0 表示发送失败，1 表示发送成功。

3.4.7.2 短信接收命令

短信接收格式和短信发送格式一样，只是 **55 AA 55 AA** 改成了 **AA 55 AA 55**。

包头	命令字	包体长度	手机号码 TLV	短信格式 TLV	短信内容 TLV	CRC
AA 55 AA 55	13	2 字节	Tag: 81 80 Length: 电话号码长度 Value: 字符串	Tag: 81 81 Length: 2 字节 Value: 当前支持 2 种格式	Tag: 81 82 Length: 短信正文长度 Value: 短信正文	2 字节

接收短信当前支持 2 种短信格式：

- **2 表示标准英文短信，**
- **3 表示标准中文短信。**

注意事项：

默认情况下短信接收功能是关闭的。如果用户想要打开，则需要在配置工具中将“DTU 工作模式设置->收短信到本地串口”从“关闭”改为“打开”。（或者用户设备自己将 0x8187 的参数配置成 0x01。）

3.5 DTU 设备的配置部分

读写配置前用户设备必须先登陆 DTU，读取状态等命令（如章节 3.4.5 ）则不需要先登陆。

3.5.1 读取 DTU 的配置

命令字：0x02

用户设备：**55 AA 55 AA 02 00 00 CD 3F**

回应命令字：0x82

包头	命令字	包体长度	TLVs	版本信息	CRC

DTU：**AA 55 AA 55 82 03 58** 81 **00 00 0F 44 47 33 31 32 31 34 30 31 39 38 37 36 37 38 … …49 6E 44 54 55 33 58 58 5F 53 54 44 5F 56 31 2E 32 2E 32 36 20 4D 61 79 20 31 33 20 32 30 31 34 20 31 39 3A 32 31 3A 33 35 06 38** DTU 回应部分包体部分包括所有 DTU 中配置的 TLV，TLV 后面跟 DTU 版本信息（软件版本号）的 ASCII 表示。

注意事项：

对这个特殊的命令，包体的长度只包含 TLVs 部分的长度，不包含版本信息部分的长度。本例中，包体长度是 0x0358, TLVs 只列了 0x8100 这个 Tag，后面还有很多 TLV 没有列全，以省略号显示。其中，**49 6E 44 54 55 33 58 58 5F 53 54 44 5F 56 31 2E 32 2E 32 36 20 4D 61 79 20 31 33 20 32 30 31 34 20 31 39 3A 32 31 3A 33 35** 是版本信息，即“InDTU3XX_STD_V1.2.26 May 13 2014

19:21:35”。

3.5.2 读取指定配置

读取指定配置，用户设备下发的数据包中包含需要读取配置的 TAG 值，TLV 的 Length 置为 0x0000，DTU 则读取相应 TAG 的 Value 回应给用户设备

命令字：0x16

包头	命令字	包体长度	TLVs	CRC

例如，读取 TAG 为 0x0001（拨号号码，详见：附录 2：配置项的 TAG 描述）的配置：

用户设备：**55 AA 55 AA 16 00 04 00 01 00 00 92 2D**

回应命令字：0x16

包头	命令字	包体长度	TLVs	CRC

DTU：**AA 55 AA 55 16 00 0C 00 01 00 08 2A 39 39 2A 2A 2A 31 23 AD 0B**

DTU 回应部分包体部分包括指定 TAG 的配置值。

3.5.3 设置 DTU 的配置

命令字：0x01

包头	命令字	包体长度	TLVs	CRC

用户设备：**55 AA 55 AA 01 03 02 00 01 00 08 2A 39 39 2A 2A 2A 31 23 … … 8A D1** 本例中，包体长度是 0x0302，TLVs 只列了 0x0001 这个 Tag，后面还有很多 TLV 没有列全，以省略号显示。

回应命令字：0x81

包头	命令字	包体长度	TLVs	CRC

DTU：**AA 55 AA 55 81 03 58 81 00 00 0F 44 47 33 31 32 31 34 30 31 39 38 37 36 37 38 … …06 38**

DTU 回应部分包体部分包括所有 DTU 中配置的 TLV，本例中，包体长度是 0x0358，TLVs 只列了 0x8100 这个 Tag，后面还有很多 TLV 没有列全，以省略号显示。

3.5.4 设置单个配置

命令字：0x18

包头	命令字	包体长度	TLVs	CRC

设置 TAG 为 0x0001 的配置：

用户设备：**55 AA 55 AA 18 00 0C 00 01 00 08 2A 39 39 2A 2A 2A 31 23 E2 B8**

回应命令字：0x18

包头	命令字	包体长度	TLVs	CRC

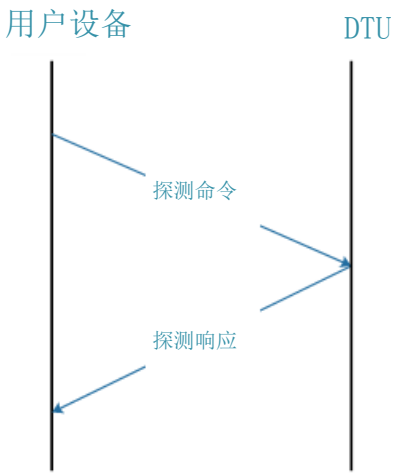
DTU：**AA 55 AA 55 18 00 0C 00 01 00 08 2A 39 39 2A 2A 2A 31 23 AD 0B**

DTU 回应包的包体部分为设置后的相应的 DTU 配置。

4. 流程描述

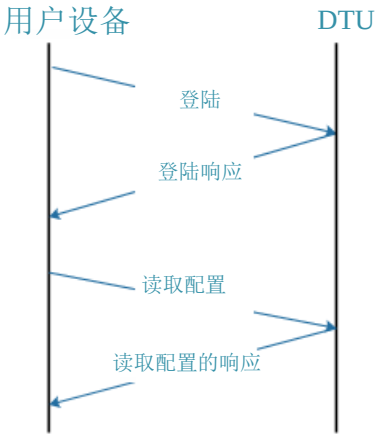
4.1 探测

任意时刻均可发起探测



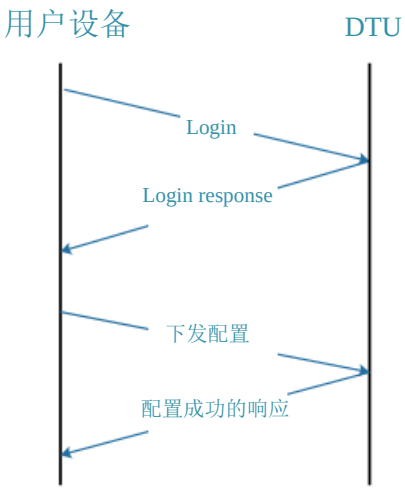
4.2 读取配置

读取配置均需要在登录状态



4.3 下发配置

下发配置需要在登录状态



5. 附录

5.1 附录 1：CRC16 源码

```
const static
unsigned short fcsTab[256] = {
        0x0000, 0x1189, 0x2312, 0x329b, 0x4624, 0x57ad, 0x6536, 0x74bf,
        0x8c48, 0x9dc1, 0xaf5a, 0xbed3, 0xca6c, 0xdbe5, 0xe97e, 0xf8f7,
        0x1081, 0x0108, 0x3393, 0x221a, 0x56a5, 0x472c, 0x75b7, 0x643e,
        0x9cc9, 0x8d40, 0xbfdb, 0xae52, 0xdaed, 0xcb64, 0xf9ff, 0xe876,
        0x2102, 0x308b, 0x0210, 0x1399, 0x6726, 0x76af, 0x4434, 0x55bd,
        0xad4a, 0xbcc3, 0x8e58, 0x9fd1, 0xeb6e, 0xfae7, 0xc87c, 0xd9f5,
        0x3183, 0x200a, 0x1291, 0x0318, 0x77a7, 0x662e, 0x54b5, 0x453c,
        0xbdcb, 0xac42, 0x9ed9, 0x8f50, 0xfbef, 0xea66, 0xd8fd, 0xc974,
        0x4204, 0x538d, 0x6116, 0x709f, 0x0420, 0x15a9, 0x2732, 0x36bb,
        0xce4c, 0xdfc5, 0xed5e, 0xfcd7, 0x8868, 0x99e1, 0xab7a, 0xbaf3,
        0x5285, 0x430c, 0x7197, 0x601e, 0x14a1, 0x0528, 0x37b3, 0x263a,
        0xdecd, 0xcf44, 0xfddf, 0xec56, 0x98e9, 0x8960, 0xbbfb, 0xaa72,
        0x6306, 0x728f, 0x4014, 0x519d, 0x2522, 0x34ab, 0x0630, 0x17b9,
        0xef4e, 0xfec7, 0xcc5c, 0xddd5, 0xa96a, 0xb8e3, 0x8a78, 0x9bf1,
        0x7387, 0x620e, 0x5095, 0x411c, 0x35a3, 0x242a, 0x16b1, 0x0738,
        0xffcf, 0xee46, 0xdcdd, 0xcd54, 0xb9eb, 0xa862, 0x9af9, 0x8b70,
        0x8408, 0x9581, 0xa71a, 0xb693, 0xc22c, 0xd3a5, 0xe13e, 0xf0b7,
        0x0840, 0x19c9, 0x2b52, 0x3adb, 0x4e64, 0x5fed, 0x6d76, 0x7cff,
        0x9489, 0x8500, 0xb79b, 0xa612, 0xd2ad, 0xc324, 0xf1bf, 0xe036,
        0x18c1, 0x0948, 0x3bd3, 0x2a5a, 0x5ee5, 0x4f6c, 0x7df7, 0x6c7e,
        0xa50a, 0xb483, 0x8618, 0x9791, 0xe32e, 0xf2a7, 0xc03c, 0xd1b5,
        0x2942, 0x38cb, 0x0a50, 0x1bd9, 0x6f66, 0x7eef, 0x4c74, 0x5dfd,
        0xb58b, 0xa402, 0x9699, 0x8710, 0xf3af, 0xe226, 0xd0bd, 0xc134,
        0x39c3, 0x284a, 0x1ad1, 0x0b58, 0x7fe7, 0x6e6e, 0x5cf5, 0x4d7c,
        0xc60c, 0xd785, 0xe51e, 0xf497, 0x8028, 0x91a1, 0xa33a, 0xb2b3,
        0x4a44, 0x5bcd, 0x6956, 0x78df, 0x0c60, 0x1de9, 0x2f72, 0x3efb,
        0xd68d, 0xc704, 0xf59f, 0xe416, 0x90a9, 0x8120, 0xb3bb, 0xa232,
        0x5ac5, 0x4b4c, 0x79d7, 0x685e, 0x1ce1, 0x0d68, 0x3ff3, 0x2e7a,
        0xe70e, 0xf687, 0xc41c, 0xd595, 0xa12a, 0xb0a3, 0x8238, 0x93b1,
        0x6b46, 0x7acf, 0x4854, 0x59dd, 0x2d62, 0x3ceb, 0x0e70, 0x1ff9,
        0xf78f, 0xe606, 0xd49d, 0xc514, 0xb1ab, 0xa022, 0x92b9, 0x8330,
        0x7bc7, 0x6a4e, 0x58d5, 0x495c, 0x3de3, 0x2c6a, 0x1ef1, 0x0f78
```

```
    };

/*
* Calculate a new fcs given the current fcs and the new data.
*/
unsigned short pppfcs16(unsigned short fcs, unsigned char *cp, unsigned short len)
{
        while (len--){
            fcs = (fcs >> 8) ^ fcsTab[(fcs ^ *cp++) & 0xff];
        }

        return (fcs);
}
//This function adds the CRC value to the two bytes following buf.
unsigned char byAddCrc16(unsigned char *cp, unsigned short len)
{
    unsigned short trialfcs;

    /* add on output */
    trialfcs = pppfcs16( 0xFFFF, cp, len );
    trialfcs ^= 0xffff;                     /* complement */
    cp[len] = (trialfcs & 0x00ff);          /* least significant byte first */
    cp[len+1] = ((trialfcs >> 8) & 0x00ff);

    return 0;
}
```

5.2 附录 2：配置项的 TAG 描述

组	名称	TAG	长度	格式	VALUE
本地串口	波特率	0x0011	2	HEX	{9600,300,600,1200,2400,4800,9600,14400,19200,38400,56000,57600,115200}; 不同数值代表表中不同波特率，从 0x00 到 0x0C.如：19200 为 0x0008， 300、600、56000 波特率在 DTU3XX 中不支持
	数据位	0x0012	1	HEX	内容即表示为数据位，如：8 为即 0x08，DTU3XX 中只支持 8 位
	停止位	0x0013	1	HEX	0x00 表示 1 位停止位，0x01 表示 1.5 停止位，0x02 表示 2 位停止位
	校验位	0x0014	1	HEX	0x00 无校验（默认），0x01 奇校验，0x02 偶校验
	扫描间隔	0x0015	2	HEX	单位为 100ms，范围 1-100。如：设置 200ms 的扫描间隔，内容即 0x02 程序以配置的串口扫描间隔作为分帧判断依据
	数据响应超时	0x0017	1	HEX	单位为秒，范围 1-255。
	帧大小	0x8118	6	HEX	单位为字节，范围 10-1024。如设置帧大小为 500 字节，内容即 0x01F4 如果在串口扫描间隔内收到超过此大小数据则强行分帧
	流控	0x0007	1	HEX	0x00 关闭（默认），0x01 打开，只有部分版本如 InDTU325 支持流控
本地串口 2	波特率	0x815C	2	HEX	{9600,300,600,1200,2400,4800,9600,14400,19200,38400,56000,57600,115200}; 不同数值代表表中不同波特率，如：19200 为 0x0008， 300、600、56000 波特率在 DTU3XX 中不支持 注意，此波特率只有在 TCP_SERVER 功能中才使用，在 TCP_SERVER 功能不打开的时候，串口 2 作为维护串口固定使用 115200 波特率
	数据位	0x815D	1	HEX	内容即表示为数据位，如：8 为即 0x08，DTU3XX 中只支持 8 位
	停止位	0x815E	1	HEX	0x00 表示 1 位停止位，0x01 表示 1.5 停止位，0x02 表示 2 位停止位
	校验位	0x815F	1	HEX	0x00 无校验（默认），0x01 奇校验，0x02 偶校验
	扫描间隔	0x8160	2	HEX	单位为 100ms，范围 1-100。如：设置 200ms 的扫描间隔，内容即 0x02 程序以配置的串口扫描间隔作为分帧判断依据
	数据响应超时	0x8162	1	HEX	单位为秒，范围 1-255
	帧大小	0x8161	6	HEX	单位为字节，范围 10-1024。如设置帧大小为 500 字节，内容即 0x01F4
DTU 工作模式	连接方式	0x001E	1	HEX	0x00 表示长连接(实时在线)，0x01 表示短连接（按需拨号）
	电话激活	0x8005	1	HEX	0x00 表示不使用电话激活，0x01 表示使用电话激活
	短信激活	0x8006	1	HEX	0x00 表示不使用短信激活，0x01 表示使用短信激活
	数据激活	0x8007	1	HEX	0x00 表示不使用数据激活，0x01 表示使用数据激活
	定时激活时间	0x8008	2	HEX	单位分，范围 5-1440，如：定时每 5 分钟激活则参数为 0x05

	间隔				
	定时下线时间间隔	0x8009	1	HEX	单位分，范围 1-60，如：串口 10 分钟没有数据即断开连接则参数为 0x0A
	GPRS 和 SMS 选择	0x818A	1	HEX	0x00 表示 GPRS 模式（默认），0x01 表示 SMS 模式
	收短信到本地串口	0x8187	1	HEX	0x00 表示关闭（默认），0x01 表示打开（参见上文收发短信部分介绍）
	DTU 配置模式	0x818B	1	HEX	0x00 表示配置数据按帧检测（默认），0x01 表示配置数据按流检测
GPRS 拨号参数	自动拨号	0x0006	1	HEX	0x01 表示自动拨号，0x00 表示不自动拨号，不自动拨号时仅使用 DM 短信激活才能让 DTU 开始拨号，默认配置为自动拨号 若未特别说明，普通用户请使用默认值
	拨号号码	0x0001	32	ASCII	拨号号码的 ASCII 表示，如配置为 12345，内容即：0x3132333435
	接入点名称 APN	0x0002	32	ASCII	APN 的 ASCII 表示
	拨号用户名	0x0003	32	ASCII	拨号用户名的 ASCII 表示
	拨号密码	0x0004	32	ASCII	拨号密码的 ASCII 表示
	PPP 层心跳间隔	0x8003	2	HEX	单位秒，范围 30-3600，若配置为 50 秒则参数为 0x0032 若未特别说明，普通用户请使用默认值
	重拨间隔	0x8116	2	HEX	单位秒，范围 0-3600，若配置为 60 秒则参数为 0x003C 若未特别说明，普通用户请使用默认值
	最大重拨次数	0x8117	1	HEX	范围 1-10，即 DTU 重拨检测模块最大连续失败多少次则重启
	认证模式	0x818D	1	HEX	0x00 自动（默认），0x01 PAP 认证，0x02 CHAP 认证 当前最新标准版程序中，自动的逻辑是使用 PAP 认证，若失败则下一次使用 CHAP 认证，若再失败则下一次使用 PAP 认证，依次循环
支撑平台相关设置	短信中心号码	0x800B	16	ASCII	短信中心号码的 ASCII 在当前最新标准版程序中，短信中心号码已经可以从 SIM 卡中自动读取到。如果从 SIM 卡中读取短信中心号码成功则使用 SIM 卡中读到的号码，如果读取失败则使用此配置项的号码
企业网关相关设置	DTU 设备号	0x0023	16	ASCII	设备号的 ASCII（DC 协议中使用）
	企业网关地址	0x0019	6	HEX	共 6 位 HEX，前 4 为表示 IP，后 2 位表示 PORT，若地址为 1.2.3.4.1024 则参数为 0x010203040400(若配置 IP 请将域名配置为空)
	企业网关域名	0x8123	32	ASCII	域名的 ASCII(若配置域名请将 IP 配置为 0.0.0.0)
	企业网关连接方式	0x001A	1	HEX	0x00 表示纯 TCP 方式，0x01 表示纯 UDP，0x03 表示 DCUDP，0x04 表示 DCTCP，0x05 表示 MODBUS 网桥方式，0x06 表示 101 转短信方式

	传输失败最大允许重发次数	0x0018	1	HEX	范围 1-5
	强制 DC 心跳	0x819E	1	HEX	0x00 关闭（默认）则心跳间隔内有数据不发送 DC 心跳，0x01 打开
	企业网关心跳间隔（分）	0x8004	1	HEX	单位分，范围 0-60
	企业网关心跳间隔（秒）	0x801F	1	HEX	单位秒，范围 0-60
	DNS1	0x8019	4	HEX	若设置为 8.8.8.8 则参数为 0x08080808
	DNS2	0x801A	4	HEX	若设置为 8.8.8.8 则参数为 0x08080808
	SNTP 服务器 IP	0x81CF	4	HEX	若设置为 8.8.8.8 则参数为 0x08080808
	本地串口互换	0x8068	1	HEX	0x00 关闭（默认），0x01 打开，默认企业网关使用串口 1,TCP server 使用串口 2，互换后企业网关使用串口 2，TCP server 使用串口 1
	TCP 服务器监听端口	0x8018	5	ASCII	范围 0-65535,0 表示不启用 TCP server 功能，如设置为 6666 则参数为 0x36363636
多中心设置	扩展 1 企业网关地址	0x800D	6	HEX	共 6 位 HEX，前 4 为表示 IP，后 2 位表示 PORT，若地址为 1.2.3.4.1024 则参数为 0x010203040400(若配置 IP 请将域名配置为空)
	扩展 1 企业网关域名	0x8124	32	ASCII	域名的 ASCII(若配置域名请将 IP 配置为 0.0.0.0)
	扩展 2 企业网关地址	0x800F	6	HEX	共 6 位 HEX，前 4 为表示 IP，后 2 位表示 PORT，若地址为 1.2.3.4.1024 则参数为 0x010203040400(若配置 IP 请将域名配置为空)
	扩展 2 企业网关域名	0x8125	32	ASCII	域名的 ASCII(若配置域名请将 IP 配置为 0.0.0.0)
	扩展 3 企业网关地址	0x8011	6	HEX	共 6 位 HEX，前 4 为表示 IP，后 2 位表示 PORT，若地址为 1.2.3.4.1024 则参数为 0x010203040400(若配置 IP 请将域名配置为空)
	扩展 3 企业网关域名	0x8126	32	ASCII	域名的 ASCII(若配置域名请将 IP 配置为 0.0.0.0)
	扩展 4 企业网关地址	0x8013	6	HEX	共 6 位 HEX，前 4 为表示 IP，后 2 位表示 PORT，若地址为 1.2.3.4.1024 则参数为 0x010203040400(若配置 IP 请将域名配置为空)
	扩展 4 企业网	0x8127	32	ASCII	域名的 ASCII(若配置域名请将 IP 配置为 0.0.0.0)

	关域名				
多连接策略	重连最小间隔	0x8015	4	ASCII	单位秒，范围 15-60，如设置为 15 秒则参数为 0x3135
	重连最大间隔	0x8016	4	ASCII	单位秒，范围 15-60，如设置为 15 秒则参数为 0x3135 重连最大间隔必须大于等于重连最小间隔，TCP 重连时使用
	轮询模式	0x8017	1	ASCII	Y 或 y 表示多中心轮询模式，N 或其他表示多中心并发模式
其他配置	最大登录次数	0x801B	1	HEX	范围 0-255，登陆超过此次数则重新连接中心
	是否允许远程 telnet	0x8163	1	HEX	0x00 表示打开远程控制台，0x01 表示关闭远程控制台，DTU3XX 中不支持此功能
	是否为调试模式	0x801D	1	HEX	0x00 表述关闭日志输出（默认），0x01 表示本地串口 1 输出日志，0x02 表示本地串口 2 输出日志，0x03 表示本地串口 5 输出日志
	调试模式等级	0x8069	1	HEX	0x00 显示详细日志（默认），0x01 中文简洁日志，0x02 英文简洁日志
	低功耗模式	0x8165	1	HEX	范围 1-8，该值表示 GPRS 上下行通道数量，0x01 一上一下功耗最低，适用于功耗要求高，数据量不大的场所，0x08 为 5 上 3 下功耗最高，适用于功耗无要求，数据量较大的场所
网管平台相关设置	产品序列号	0x8100	16	ASCII	该值为每个 DTU 唯一固定值，不可更改
	工作模式	0x810B	1	HEX	0x00 表示关闭 DM 平台，0x01 表示仅短信，0x02 表示短信+IP 模式
	信任号码列表（逗号分隔）	0x810D	64	ASCII	信任号码的 ASCII，如需要配置多个网管平台信任号码，则每个号码间用逗号分隔，如 15901003379,15901003379，最长 64 字节
	设备号	0x8101	4	HEX	该设备号为每个 DTU 唯一固定，不可更改
	网管平台地址	0x810E	6	HEX	共 6 位 HEX，前 4 为表示 IP，后 2 位表示 PORT，若地址为 1.2.3.4.1024 则参数为 0x010203040400
	网管平台心跳间隔	0x8105	2	HEX	单位秒，范围 30-600
ICMP 参数设置	ICMP 探测主机	0x8119	4	HEX	4 位 HEX 表示 IP 中的 4 段
	ICMP 最大丢包数	0x8115	1	HEX	范围 3-60
	网络空闲间隔	0x811A	2	HEX	单位秒，范围 30-3600
	强制 ICMP 探测	0x819D	1	HEX	0x00 关闭（默认），0x01 打开 关闭时，则任何收到网络数据都会重新开始计时，累计达到网络空闲间隔时才发送 ICMP 探测包，连续累计达到 ICMP 最大丢包数则会重新拨号；打开时，无论是否收到网络数据，累计达到网络空闲间隔就一定会发送 ICMP 探测包，连续累计达到 ICMP 最大丢包数则会重新拨号
自定	登录帧	0x8174	1	HEX	0x00 表示 ASCII，0x01 表示 HEX，0x02 表示 DC 格式包

义帧	类型				
	登陆帧	0x811D	64	随类型值变化	设置为 ASCII 时填写任意字符， 设置 HEX 时每两字节组成 1 字节数据例如 0x31,0x32 两字节数据拼接成 0x12 这一个字节，也就是说 HEX 格式时实际发送最长为 64/2=32 字节，设置 DC 时不需要填写，因为 DC 有自己的格式
	登录回应帧类型	0x8175	1	HEX	0x00 表示 ASCII，0x01 表示 HEX，0x02 表示 DC 格式包
	登录回应帧	0x811E	64	随类型值变化	设置为 ASCII 时填写任意字符， 设置 HEX 时每两字节组成 1 字节数据例如 0x31,0x32 两字节数据拼接成 0x12 这一个字节，也就是说 HEX 格式时实际发送最长为 64/2=32 字节，设置 DC 时不需要填写，因为 DC 有自己的格式
	心跳帧类型	0x8178	1	HEX	0x00 表示 ASCII，0x01 表示 HEX，0x02 表示 DC 格式包
	心跳帧	0x8121	64	随类型值变化	设置为 ASCII 时填写任意字符， 设置 HEX 时每两字节组成 1 字节数据例如 0x31,0x32 两字节数据拼接成 0x12 这一个字节，也就是说 HEX 格式时实际发送最长为 64/2=32 字节，设置 DC 时不需要填写，因为 DC 有自己的格式
	心跳回应帧类型	0x8179	1	HEX	0x00 表示 ASCII，0x01 表示 HEX，0x02 表示 DC 格式包
	心跳回应帧	0x8122	64	随类型值变化	设置为 ASCII 时填写任意字符， 设置 HEX 时每两字节组成 1 字节数据例如 0x31,0x32 两字节数据拼接成 0x12 这一个字节，也就是说 HEX 格式时实际发送最长为 64/2=32 字节，设置 DC 时不需要填写，因为 DC 有自己的格式
	退出帧类型	0x8176	1	HEX	0x00 表示 ASCII，0x01 表示 HEX，0x02 表示 DC 格式包
	退出帧	0x811F	64	随类型值变化	设置为 ASCII 时填写任意字符， 设置 HEX 时每两字节组成 1 字节数据例如 0x31,0x32 两字节数据拼接成 0x12 这一个字节，也就是说 HEX 格式时实际发送最长为 64/2=32 字节，设置 DC 时不需要填写，因为 DC 有自己的格式
	退出回应帧类型	0x8177	1	HEX	0x00 表示 ASCII，0x01 表示 HEX，0x02 表示 DC 格式包
	退出回应帧	0x8120	64	随类型值变化	设置为 ASCII 时填写任意字符， 设置 HEX 时每两字节组成 1 字节数据例如 0x31,0x32 两字节数据拼接成 0x12 这一个字节，也就是说 HEX 格式时实际发送最长为 64/2=32 字节，设置 DC 时不需要填写，因为 DC 有自己的格式
短信相关	短信号码	0x8180	16	ASCII	接收/发送手机号码的 ASCII
	短信类型	0x8181	1	HEX	0x00 表示定制英文短信，0x01 表示定制中文短信，0x02 表示标准英文短信，0x03 表示标准中文短信
	短信内容	0x8182	140 /160	随内容变化	英文短信时为 ASCII，最长 160 字节，中文短信时为 Unicode 码，最长 140 字节，中文标准短信“你好”占用 4 字节(0x4F 0x60 0x59 0x7D)
	短信回执	0x8189	1	HEX	0x00 表示发送失败，0x01 表示发送成功，0x02 表示收到正确的短信数据帧

5.3 附录 3：状态项的 TAG 描述

组	名称	TAG	长度	内容格式	描述
老版协议	DTU 当前工作状态	0x8183	1	HEX	0x01 表示初始化中，0x02 表示正在拨号，0x03 拨号成功但未连接中心，0x04 表示连接主站成功
	信号值（CSQ）	0x8184	1	HEX	范围 0~31，或者 99（表示无信号），0x1F 表示 CSQ 为 31.
物理层状态	IMEI	0x81CA	15	ASCII 值	表示和通讯模块一一对应的 IMEI 码
	IMSI	0x81CB	15	ASCII 值	表示和 SIM 卡一一对应的 IMSI 码
	ICCID	0x81D0	20	ASCII 值	表示和 SIM 卡一一对应的 ICCID 码(一般会标注在 SIM 卡的背面)
	信号值（CSQ）	0x819F	2	HEX	范围 0~31，或者 99（表示无信号），0x001F 表示 CSQ 为 31.
	频段	0x81A0	2	HEX	可能值为 900,1800,2100
	注册状态	0x81A1	2	HEX	0x00 表示未注册，0x01 表示已注册（本地），0x05 表示已注册（漫游）
	MCC	0x81A3	2	HEX	表示 DTU 当前运营商的移动国家码，中国为 460（0x01CC）
	MNC	0x81A4	2	HEX	表示当前运营商的移动网络码，如 MNC 为 00,MCC 为 460 表示中国移动
	LAC	0x81A5	2	HEX	表示 DTU 所在网络基站的位置区码
	CELL ID	0x81A2	2	HEX	表示 DTU 所在网络基站的扇区区码
	重启信息	0x81A6	2	HEX	0x00 表示硬重启，0x01 表示软重启
网络层状态	认证方式	0x81A7	2	HEX	0x00 表示 PAP 认证，0x01 表示 CHAP 认证
	IP 地址	0x81A8	4	HEX	4 字节 HEX 表示 DTU 拨号得到的 IP 中的 4 段
	接收流量	0x81A9	4	HEX	IP 包的接收总字节数
	发送流量	0x81AA	4	HEX	IP 包的发送总字节数
	LCP 延时	0x81AC	2	HEX	LCP 的实时延时
	PPP 状态	0x81AD	2	HEX	PPP 状态,0x00 表示拨号未成功，0x01 表示拨号已成功
	PING 延时	0x81AB	2	HEX	PING 的实时延时
	PING 丢包率	0x81AE	2	HEX	PING 包的丢包率
应用层状态	中心 1 连接状态	0x81B1	2	HEX	0x00 表示未连接，0x01 表示已连接
	中心 1 延时	0x81AF	2	HEX	表示 DC 心跳包的实时延时
	中心 1 丢包率	0x81B0	2	HEX	表示 DC 心跳包的丢包率
	中心 2 连接状态	0x81B4	2	HEX	0x00 表示未连接，0x01 表示已连接
	中心 2 延时	0x81B2	2	HEX	表示 DC 心跳包的实时延时
	中心 2 丢包率	0x81B3	2	HEX	表示 DC 心跳包的丢包率
	中心 3 连接状态	0x81B7	2	HEX	0x00 表示未连接，0x01 表示已连接
	中心 3 延时	0x81B5	2	HEX	表示 DC 心跳包的实时延时
	中心 3 丢包率	0x81B6	2	HEX	表示 DC 心跳包的丢包率
	中心 4 连接状态	0x81BA	2	HEX	0x00 表示未连接，0x01 表示已连接
	中心 4 延时	0x81B8	2	HEX	表示 DC 心跳包的实时延时
	中心 4 丢包率	0x81B9	2	HEX	表示 DC 心跳包的丢包率
	中心 5 连接状态	0x81BD	2	HEX	0x00 表示未连接，0x01 表示已连接
	中心 5 延时	0x81BB	2	HEX	表示 DC 心跳包的实时延时

	中心 5 丢包率	0x81BC	2	HEX	表示 DC 心跳包的丢包率
	中心 1 掉线重连次数	0x8320	2	HEX	表示与中心 1 的连接断开后重连的次数
	中心 2 掉线重连次数	0x8321	2	HEX	表示与中心 2 的连接断开后重连的次数
	中心 3 掉线重连次数	0x8322	2	HEX	表示与中心 3 的连接断开后重连的次数
	中心 4 掉线重连次数	0x8323	2	HEX	表示与中心 4 的连接断开后重连的次数
	中心 5 掉线重连次数	0x8324	2	HEX	表示与中心 5 的连接断开后重连的次数