数据采集记录仪与远程服务器通信协议

一、基本定义

主机：运行在服务器上的软件服务(云平台)。

设备：与软件平台进行直接交互的单一节点的硬件设备，例如数据采集记录仪、控制器、传感器等，不包含转发网关。

传输方式：基于 TCP/IP 的 GPRS、NB-IoT、WLAN 等网络传输。

协议格式：TLV 格式、自定义格式。

设备 ID：作为设备与主机通讯时的唯一标识，是一个由大/小写字母、数字和下划线组成的长度不超过 16B 的字符串。

1B：表示 1 个字节。

4b：表示 4 个二进制位。

✧ *留意区分本文档协议报文中各个字段的底色，有助于对协议结构的理解。*

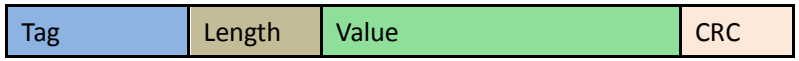
✧ *说明和样例中带单引号的字段为 ASCII 表示，实际传输内容是不包含这些单引号的；不带单引号的部分均为十六进制数据表示。*

二、协议格式

2.1 TLV 协议概述

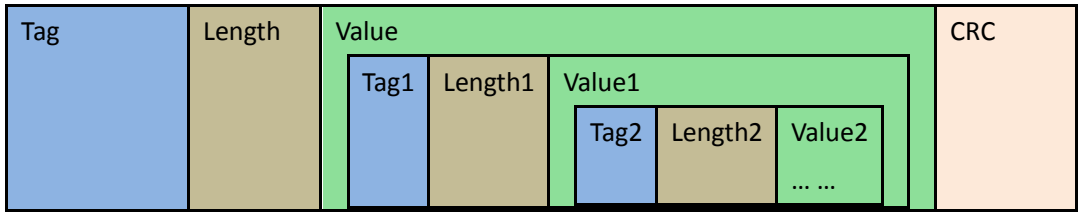
TLV 通信协议，即 Tag-Length-Value，是一种简单实用的数据传输方案。在 TLV 的定义中，可以知道它包括三个域，分别为：标签域(Tag)、长度域(Length)、内容域(Value)，各域紧密相连。TLV 协议可级联，可嵌套。

基本格式为



带有级联的格式为

带有嵌套的格式为



2.2 TLV 各域说明

2.2.1 标签域(Tag)

长度为 1B，在本通信协议中的功能描述如下表(Tag 的值区分大小写)：

Tag 值	功能	说明
‘A’	设备主动上报数据时作为帧头	
‘#’	上报数据时数据内容区域的分隔标签	
‘Q’	主机发起数据采集	
‘C’	配置设备运行参数	修改设备运行期间的参数，例如数据上报的时间间隔
‘N’	配置设备联网参数	包含目标地址、端口、接入点等信息
‘@’	心跳包的帧头	

2.2.2 长度域(Length)

表示其后面内容域的字节数，长度为 1B。

2.2.3 内容域(Value)

表示何种功能意义，和占用多少字节数分别由其前的标签域和长度域所定义。

2.2.4 校验域(CRC)

校验域仅出现在一条完整的报文的末尾，对前面所有内容进行 CRC 计算。带有级联或嵌套格式的，各个级联或嵌套内 TLV 的末尾不加本校验。使用 CRC16-MODBUS 计算方法，长度为 2B，低字节在前，高字节在后。

三、协议详解与样例

下面以一台水质五参数监测终端(设备)为例，对通信协议的具体格式和功能意义，结合样例进行说明。

3.1 数据上报包

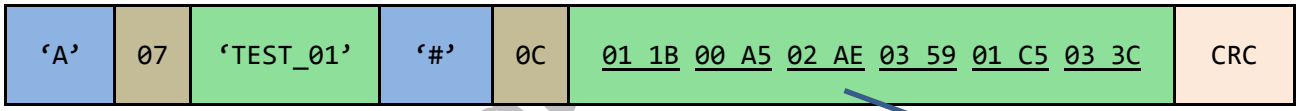
用于设备对主机进行采集数据上报之用。分为以下两种实现方式：

3.1.1 主动上报

即设备按某些条件，例如预设的定时周期或某些测量值变化触发条件，自动上报数据。该方式在低功耗物联网数据采集中最为常用。

例如，某个监测终端共上报 6 个测量要素，依序分别为温度、电导率、pH、溶解氧浓度、浊度、设备电压。设备每次上报数据的格式及样例如下：

(设备->主机)

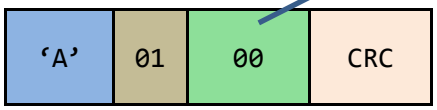


在数据内容中，每个测量要素占用固定的 2B 长度，且顺序也是固定的

报文的形式为一个二级级联的 TLV。

本例表示该设备的设备 ID 为”TEST_01”，上报参数的内容为温度 28.3℃，电导率 1.65mS/cm，pH 6.86，溶解氧浓度 8.57mg/L，浊度 453NTU，设备电压 8.28V。

主机收到报文并尝试解析后，应答解析结果代码：(主机->设备)

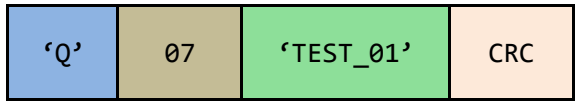


0- 解析成功
1- 长度不完整
2- 校验失败
3- 数据格式有误

3.1.2 被动查询

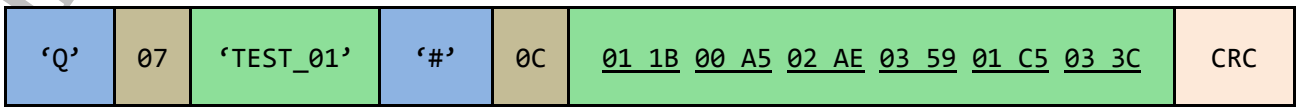
在这种方式下，需要设备一直处于工作且可通讯的状态，每次通讯由主机发起。主机询问设备 ID，相应的设备应答测量数据。

(主机->设备)



本例表示，主机将要查询设备 ID 为“TEST_01”的测量数据，设备应答如下：

(设备->主机)



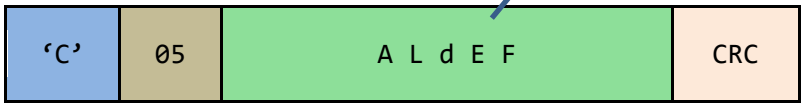
本报文除帧头不同外，解析和应答的方法与 3.1.1 相同。

3.2 设备配置包

3.2.1 配置写入运行参数

(主机->设备)

此处用一个字母代表一个参数，每参数占用 1B，均为数值



A 数据采集频次(见下表)

L 数据记录/上报频次，不得快于数据采集频次(见下表)

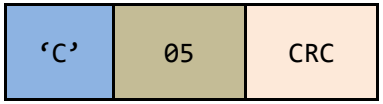
值	意义
0	5 秒
1	10 秒
2	半分钟
3	1 分钟
4	5 分钟
5	15 分钟
6	半小时
7	1 小时
8	2 小时
9	每天的 0，6，12，18 点整
10	每天的早晚 8 点整
11	每天的 0 点整

d 采集前对传感器的上电预热时长，单位 s

E 数据采集后是否存储入机身：1-存储 0-不存储

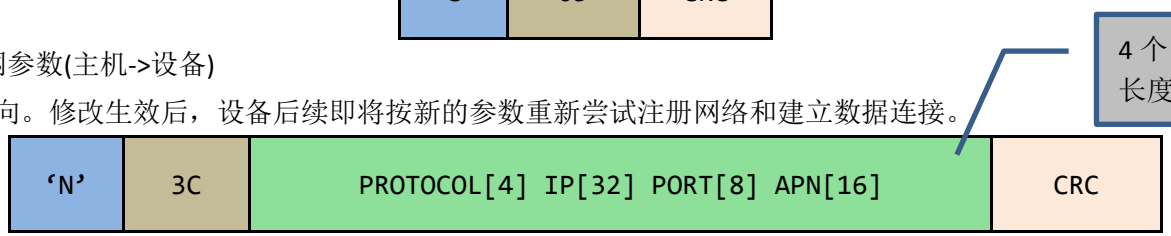
F 记录存储模式：0-顺序模式，即存满后停止记录 1-循环模式，即存满后回到初始地址滚动存储

设备收到报文并正确解析后，应答刚才收到内容的主 T 域和主 L 域(注意更新校验域)：(设备->主机)



3.2.2 配置写入无线联网参数(主机->设备)

用于修改设备的连接指向。修改生效后，设备后续即将按新的参数重新尝试注册网络和建立数据连接。



PROTOCOL[4] 网络协议，’TCP’或者’UDP’，后面再填充 1 个’\0’，补足 4B。

IP[32] 目标主机地址，即设备所连接远程服务器(软件平台即运行在该服务器上)的 IP 地址字符串或者域名字符串。同理后面用'\0'补足 32B。

PORT[8] 目标端口，运行在服务器上的数据接收服务开启的监听端口，字符串，同理后面用'\0'补足 8B。

APN[16] 网络接入点名称。该内容为按需设置，一般设置为空白即可(即 16 个'\0')，此时设备将自动获取 APN。除非比如使用了海外运营商或接入特殊单位的内部网络(设备端同时应注意 SIM 卡是否支持)。

设备应答格式同 3.2.1。

3.3 心跳包

用于设备与主机首次建立连接，相互交互信息，以及维持连接的目的(定时发送)。由设备主动发起，格式如下：

(设备->主机)

'@'	07	'TEST_01'

或者当设备配置有全球定位功能时，格式为二级级联 TLV 如下：

(设备->主机)

'@'	07	'TEST_01'	'#'	13	'N37.99567E116.45246'

经纬度字符串，中间无空格
解析经度时，可以以前缀 N(或 S)作为识别
解析纬度时，可以以前缀 E(或 W)作为识别

设备上发心跳包不带校验域。

主机收到设备上发的心跳包后，可在自己的数据库中做 IP、端口与该设备 ID 之间的索引绑定，以便后面调用，同时对其应答下行心跳报文如下。

(主机->设备) (非 TLV 格式)

'S'	13	04	15	12	0F	37	84
帧头	年	月	日	时	分	秒	累加和校验

中间 6B 依序分别为服务器当前的年月日时分秒，最后 1B 表示对该 6B(不包含帧头)的累加和用于校验。本样例表示的时间点为 2019 年 4 月 21 日 18:15:59，可用于对设备做时钟同步。

低功耗物联网采集设备，联网为短连接，在建立连接后可能不上发心跳包，而是直接主动上报数据包，然后保持数秒的网络连接(主要是等待是否有主机发来的设备配置包)之后下线休眠，主机后续无法再通过刚才建立的套接字找到该设备。不过这类设备有时也可能按需上发一次心跳包，目的是为给自己做时钟同步。

长连接的设备，则在首次成功连接服务器后立即上发一个心跳包，之后在无通讯的时段里，一般以 1 分钟的间隔上发心跳包。

3.4 通讯报文实例

报文(HEX)	注释
40 07 54 45 53 54 5F 30 32	设备 ID 为 TEST_02 的设备上发心跳
53 13 04 12 0D 23 02 5B	服务器下发心跳 2019/4/18 13:35:02
41 07 54 45 53 54 5F 30 32 23 04 01 24 00 A3 12 47	TEST_02 设备上报一次数据，里面包含 2 个测量参数
41 01 00 20 44	服务器应答：解析成功
41 06 4C 4F 47 47 45 52 23 0A 05 3C 02 11 00	设备 ID 为 LOGGER 的设备上报一次数据，似乎有 5 个测量参数
41 01 01 E1 84	服务器应答：长度不完整
41 06 4C 4F 47 47 45 52 23 0A 05 3C 02 11 00 75 21 D6 6A C2 46 DE	设备 ID 为 LOGGER 的设备又上报一次数据，有 5 个测量参数
41 01 00 20 44	服务器应答：解析成功
43 05 09 09 0A 01 01 56 5E	服务器对该设备发送设备配置包
43 05 F0 83	设备应答成功