

AWT100 服务器对接协议

修改历史

版本	日期	作者	备注
1.0	2019-10-23		

1、基本格式

起始符 { { (2字节)	命令字(固定) (1字节)	14位网关序列号+6 位预留 (20字节)	消息体(可 变)	校验位 (2字节)	结束符 } } (2字节)
------------------------	------------------	-----------------------------	-------------	--------------	------------------------

1.1 起始符结束符

以“{{”为帧起始

以“}}”为帧结束

1.2 CRC 校验

校验位长度为2个字节，Modbus CRC 校验算法。

校验范围为命令字开始（含命令字）到消息体结束。

注：任何与服务器进行交互的数据都需要按此格式进行编解码。（包括透传，注册等等）

1.3 命令描述

功能	描述	仪表请求	服务器响应	服务器下发	仪表响应	备注
1、	对时	0x93	0x93			仪表和服务器校时
2、	Modbus 数据域上传	0x91	0x91			根据配置的数据域上传 Modbus 数据包
3、	Modbus 数据透传			0x90	0x90	服务器下发透传命令， 仪表根据 Modbus 命令 进行响应
4、	设置 IP 端口			0x88	0x88	设置服务器 IP 和端口
5、	设备注册	0x84	0x84			打开 TCP 连接后立即发 送注册包
6、	上传参数设 定值	0x89	0x89			上传参数字段
7、	设备参数下 发			0x82	0x82	含上传时间间隔

2、通信规则

仪表与服务器之间的通信采用一问一答方式。应答方需对消息包进行 CRC 校验等有效性检查，判定有效消息后才做相应应答。应答的命令字和发起方相同。应答方只做一次应答，不重复发包。

为确保消息的送达，消息发送方如果未收到消息响应，则需要在间隔一定时间后重新发送该消息，直到收到消息应答为止。

重发间隔建议设定为 1s 到 30s 之间，视消息重要性程度自由选择，但最长不超过 2 分钟。

在消息重发若干次未收到应答消息，则可判定为设备离线。设备及服务器做相应处理，其中仪表在离线后需要把离线状态在设备界面显示出来。

1、对时命令

仪表请求，命令字：0x93

服务器下发，命令字：0x93

协议描述	字段含义	字段类型	长度	描述
消息体	年	byte	1	
	月	byte	1	
	日	byte	1	
	星期	Byte	1	
	时	Byte	1	
	分	Byte	1	
	秒	Byte	1	

报文举例：

请求时间..

数据上传:

7b 7b 93 s1 s2 s3 s4 s5 s6 s7 s8 s9 s10 s11 s12 s13 s14 00 00 00 00 00 00 00 00 crc1 crc2 7d 7d

数据接收:14

7b 7b 93 12 04 10 01 0d 11 1a e6 90 7d 7d

收到时间..

2、Modbus 数据域上传

仪表发送 Modbus 数据流：命令字：0x91

协议描述	字段含义	字段类型	长度	描述
消息体	如下			例: [[1-1((0110000000crc))]] [[1-2((0110000000crc))]] [[1-3((un))]]

服务器响应：命令字：0x91

报文举例：

数据上传:

7b 7b 91 s1 s2 s3 s4 s5 s6 s7 s8 s9 s10 s11 s12 s13 s14 00 00 00 00 00 00 00 00 5b 5b 31 2d 31 28 28

第一段数据段 29 29 5d 5d 5b 5b 31 2d 32 28 28 第二段数据段 29 29 5d 5d 5b 5b 31 2d 33 28

28 第三段数据段 29 29 5d 5d 5b 5b 31 2d 34 28 28 第四段数据段 29 29 5d 5d 5b 5b 31 2d 35

28 28 第五段数据段 29 29 5d 5d crc1 crc2 7d 7d

数据接收:7

7b 7b 91 7e ec 7d 7d

3、Modbus 数据下发（透传）

服务器下发 Modbus 数据流：命令字：0x90

协议描述	字段含义	字段类型	长度	描述
消息体	Modbus 数据流	byte	不定	此处做 Modbus 帧判断

仪表响应：命令字：0x90

协议描述	字段含义	字段类型	长度	描述
消息体	Modbus 数据流	byte	不定	根据仪表回送的数据流

报文举例：

数据接收:15

7b 7b 90 请求帧 e6 fd 7d 7d

收到透传命令..

发送透传数据..

数据上传:96

7b 7b 90 s1 s2 s3 s4 s5 s6 s7 s8 s9 s10 s11 s12 s13 s14 00 00 00 00 00 00 00 回复帧 crc1 crc2 7d 7d

4、修改 IP 地址，端口，TCP 连接类型

服务器发送：命令字：0x88

协议描述	字段含义	字段类型	长度	描述
消息体	传输协议类型	byte	1	00: tcp 01: udp
	IP	byte (*)	4	IP
	Port 端口	byte (*)	2	端口号

仪表响应：命令字：0x88

协议描述	字段含义	字段类型	长度	描述
消息体	IP 修改状态	byte	1	0x00: 修改成功，重启后连接新的 IP 0x01: 修改失败

报文举例：

数据接收:14

7b 7b 88 00 3d a0 42 1a 1a df b2 7e 7d 7d

收到 IP 配置命令..

响应设置 IP 端口，启动重连..

数据上传:8

7b 7b 88 s1 s2 s3 s4 s5 s6 s7 s8 s9 s10 s11 s12 s13 s14 00 00 00 00 00 00 00 01 a6 70 7d 7d

5、设备注册

仪表发送，命令字：0x84

协议描述	字段含义	字段类型	长度	描述
消息体	注册序列号	byte	20	最长 20 个字符，字符串以'\0'作为结束，不足补零
	卡号	Byte	30	最长 30 个字符，字符串以'\0'作为结束，不足补零
	信号强度	byte	1	1~31 RSSI 信号值
	固件版本 1	byte (BCD)	2	当前固件版本
	固件版本 2	byte (BCD)	2	当前固件版本
	固件版本 3	byte (BCD)	2	当前固件版本
	定时上传间隔	Byte	1	分钟 默认为 5min

服务器响应，命令字：0x84

报文举例：

数据上传:65

7b 7b 84 s1 s2 s3 s4 s5 s6 s7 s8 s9 s10 s11 s12 s13 s14 00 00 00 00 00 00 00 00 00 38 39 38 36 30 32 42
35 30 39 31 36 30 30 33 30 33 36 32 32 00 1a 01 00 01 00 01 00 02 25
d7 7d 7d

数据接收:7

7b 7b 84 bf 23 7d 7d

6、参数设定值字段上传

服务器下发，命令字：0x89

协议描述	字段含义	字段类型	长度	描述
消息体	参数字段		不定	例: [[1-1((0110000000crc))]] [[1-2((0110000000crc))]] 0x1231 13 位, 0x102F 36 位

服务器响应，命令字：0x89

报文举例：

数据上传:137

7b 7b 89 s1 s2 s3 s4 s5 s6 s7 s8 s9 s10 s11 s12 s13 s14 00 00 00 00 00 00 00 00 00 00 00 00 5b 5b 31 2d 31 28 28
第一段参数段 29 29 5d 5d 5b 5b 31 2d 32 28 28 第二段参数段 29 29 5d 5d ed 5d 7d 7d

数据接收:7

7b 7b 89 7e e6 7d 7d

7、修改设备参数

服务器下发，命令字：0x82

协议描述	字段含义	字段类型	长度	描述
消息体	上传定时间隔	Byte	1	分钟 默认为 5min

服务器响应，命令字：0x82

报文举例：

数据接收:8

7b 7b 82 02 e0 d1 7d 7d

收到设备参数设置命令..

响应参数下发..

数据上传:8

7b 7b 82 s1 s2 s3 s4 s5 s6 s7 s8 s9 s10 s11 s12 s13 s14 00 00 00 00 00 00 00 01 a0 d0 7d 7d

仪表上电初始化流程如下：

- 1、仪表上电后主动上报注册包，收到服务器回应的注册包。
- 2、上传参数字段。
- 3、初始化完成。

正常工作流程

- 1、仪表按照定时时间主动上传数据。
- 2、有报警产生时主动上报数据域
- 3、响应服务器下发的其他指令（透传，设定参数，固件升级，等）