



# ZSDxx1x串口及远程控制协议

众联万物 智慧未来

我们用心创造

## 前 言

感谢您使用成都众山科技有限公司提供的DTU产品。

本手册主要介绍众山 ZSDxx1x、ZSDRxx1x 系列 DTU 远程控制协议。

适用型号：ZSD2110、ZSD3110、ZSD2310、ZSD3310、ZSD2410、ZSD3410、ZSD3411、ZSDR3411。

## 版权声明

本手册版权属于成都众山科技有限公司，任何人未经我公司书面同意复制将承担相应法律责任。

## 版本信息

文档名称：ZSDxx1x串口及远程控制协议

版本：1.10

修改日期：2018年12月27日

## 相关文档

- 1、《ZSDxxxx DTU Easy 控件接口说明》
- 2、《众山 DTU Modbus 协议手册》
- 3、《众山 DTU 脚本编程手册》
- 4、《ZSDxxxx 网络模式选择手册》

## 更新记录

- 1、E024命令修改为读取IMSI号码
- 2、增加E029命令读取ICCID号码

## 一、手册说明

本手册详细描述众山 DTU 的参数配置细节和 DTU 各种控制命令，使用这些协议不仅让用户可以在串口端进行 DTU 参数的修改、读取或者使用一些执行命令控制 DTU，而且在中心端也使用相同的协议对 DTU 进行同样的配置和控制。众山 DTU 在串口端接收用户数据和接收到中心下行数据满足本协议规定的数据格式时，DTU 不做透传处理，用于配置（读取）DTU 参数、控制 DTU、读取 DTU 各种状态等。

众山 DTU 协议分为两种类型，以 AA55 开始的控制协议和控制 DI/DO 的 Modbus 协议，DTU 在串口端收到 AA55 开始并且校验正确的数据包，DTU 会根据命令执行不同的操作，并不透传到数据中心，否则 DTU 会作为透传数据发送到数据中心。DTU 在收到数据中心下发的 AA55 开始并且校验正确的数据包时，也会进行相同的处理，便于用户中心控制 DTU，参数配置等，也不会透传到串口。在带有 DI/DO 的 DTU 中，DTU 还会解析 Modbus 协议，满足 Modbus 地址为自己或者广播地址时，并且 CRC 校验正确，DTU 也不会把数据进行透传。

本手册规定的协议在 DTU 串口层和任何网络模式下通用，TCP Clinet/UDP Master 或者 TCP-ZSD/UDP-ZSD。DTU 的串口配置软件就是采用此协议开发的，如果用户只需要在电脑上配置 DTU，直接使用我们提供的配置软件进行配置，即使在远程中心端，也可以把连接上中心的 DTU 虚拟成一个串口，用配置软件打开虚拟串口即可进行远程配置。如果用户需要在自己的设备或者自己的中心软件中嵌入这些功能，则可以使用本协议进行开发。

本手册规定的协议不仅可以让用户从 DTU 的串口端控制 DTU，还可以从中心服务器端远程控制 DTU，甚至用户可以把此协议中的数据包设置在 DTU 的脚本参数的 @C 命令中，让 DTU 使用此协议根据脚本定义的规则定时控制 DTU 或获取 DTU 各种状态。DTU 脚本参数的 @C 命令相当于代替用户的中心下发指令且能周期执行。详细关于使用脚本控制 DTU 的细节请参考《众山 DTU 脚本编程手册》。

本手册只描述 AA55 协议，控制 DI/DO 的 Modbus 协议请参考《众山 DTU Modbus 协议手册》。

## 二、AA55 协议介绍

### 2.1 协议格式

字节位置	名称		备注
1	AA	包头	
2	55	包头	
3	Length_H	长度高字节	从第 5 字节命令开始到最后校验所有的字节
4	Length_L	长度低字节	

			数
5	Cmd_H	命令高字节	后面详细解释各种不同的命令
6	Cmd_L	命令低字节	
7~N	Data1 . . DataN	数据	不定长数据
N+1	ACC_H	累加和校验	从第 3 字节长度开始到第 N 字节数据结束的累加和校验
N+2	ACC_L	累加和校验	

表 2.1

注：1. 所有 2 字节或 4 字节整数表示的值传输方式都是高字节在前，低字节在后

2. 累加和校验算法：除了包头和校验以外的所有字节相加，超过 FFFF 自动溢出

## 2.2 参数配置详解

参数命令	名称	参数数据长度	参数格式	默认值	备注
0030	设备 ID 号	8	字符串	“00000000”	用于在 TCP-ZSD 协议或 UDP-ZSD 协议下登录中心的 8 位 ID 号
0031	登录密码	6	字符串	“000000”	用于在 TCP-ZSD 协议或 UDP-ZSD 协议下登录中心的 6 位密码
0032	接入点名称	0~31	字符串	“CMNET”	这些参数用于 DTU 在接入专网时使用，不使用专网时按照默认配置无需修改，也不会产生影响
0033	接入点用户名			“WAP”	
0034	接入点密码			“WAP”	
0035	主 DNS IP 地址	4	HEX	08080808	在中心使用域名时需要使用，默认 8.8.8.8 和 114.114.114.114
0036	副 DNS IP 地址			72727272	
0037	自动获得 DNS	1	0 或 1	1	0：关闭 1：开启
0045	串口波特率	4-9	字符串	“9600”	支持 1200-115200 的波特率
0048	串口分包数据间隔时间	2	2-1000	2	串口数据超过时间间隔，DTU 会打包发送，单位为 0.01S，即可设置 20 毫秒~10 秒

0062	modem 模式	1	0 或 2	0	0 为 DTU 模式，2 为 modem 模式，modem 模式设备相当于一个 234G 模组，用户用 AT 命令自己开发所有功能
0040	网络模式	1	0: TCP-ZSD 1: UDP-ZSD 2: TCP Client 3:UDP Master	0	TCP-ZSD 和 UDP-ZSD 为众山 DTU 在 TCP 和 UDP 模式下增加了应用层协议，便于中心管理 DTU，需要使用众山 SDK 开发用户的数据中心，TCP Client 和 UDP Master 模式为全透明 TCP 和 UDP，在此模式下用户可以自定义登录心跳等，也可以不配置
0041	中心 IP 地址或域名	0-99	字符串	空	中心的 IP 地址或者域名，支持多中心的型号中多个中心需要使用逗号“,” 隔开
0042	中心端口	0-19	字符串	空	中心的端口号，支持多中心的型号中多个中心需要使用逗号“,” 隔开，与 IP 参数一一对应
0060	备用中心 IP 地址或域名	0-99	字符串	空	备用中心的 IP 或域名，和主中心一一对应，互为备份，当中心连不上时，轮流切换连接
0061	备用中心端口	0-19	字符串	空	备用中心端口号，与备用中心 IP 参数一一对应
0044	心跳时间	2	整数	30	心跳时间，单位为秒，0 表示不发心跳
0049	心跳模式	1	0: 无心跳 1: 发心跳，不需中心应答 2: 发心跳，需要中心应答	0	规定在 TCP Client 和 UDP Master 模式下 DTU 的心跳机制，如果设置了模式 2 需要应答，平台必须按照心跳应答包内容应答，否则 DTU 会重复发送心跳，发送几次仍未应答时 DTU 进入重连状态
004A	心跳包发送内容		1 字节长度+		TCP Client 和 UDP Master 模式下的心跳发送内容和应答内

004B	心跳包应答内容	0-31	内容	0	容, HEX 格式, 参数内容的第一个字节为参数长度, 后面为内容
0050	登录模式	1	0: 不发登录包 1: 发登录包, 不需中心应答 2: 发登录包, 需要中心应答	0	规定在 TCP Client 和 UDP Master 模式下 DTU 在连接中心后, 是否发送登录包, 如果设置了模式 2 需要应答, 平台必须按照登录应答包内容应答, 否则 DTU 会重复发送登录包, 发送几次仍未应答时 DTU 进入重连状态, 在登录包未应答之前, DTU 不进行数据透传。
004C	登录包发送内容	0-31	1 字节长度+ 内容	0	TCP Client 和 UDP Master 模式下的登录包发送内容和应答内容, HEX 格式, 参数内容的第一个字节为参数长度, 后面为内容
0051	登录包应答内容				
004D	发送数据头	0-31	1 字节长度+ 内容	0	TCP Client 和 UDP Master 模式下在 DTU 发送的数据包前插入一个自定义的头, 为空表示不插入头
004E	中心连接成功提示信息	0-31	1 字节长度+ 内容	0	中心连接成功时的提示信息
004F	中心连接断开提示信息				中心断开连接时的提示信息
0052	DTU 的 Modbus 地址	1	整数	100	在有 DI/DO 功能的 DTU 中, 用于中心 DI/DO 控制的 Modbus 地址
003F	强制心跳	1	0: 不强制心跳 1: 强制心跳	1	0: 在有数据下行时, DTU 不发心跳 1: 任何情况下,DTU 都定时心跳
0090	物联云开关	1	0: 关 1: 开	1	在物联云开关开启情况下, DTU 会连接众山的云平台, 用户需要自建中心时必须关闭物

					联云开关
0092	物联网登录密码	6	字符串	“000000”	登录众山物联网密码
F000	调试模式	1	0: 关 1~15:调试级别	0	当调试模式为 10 以上时，DTU 输出详细的调试信息，用于 DTU 排查问题，用户正常使用时请关闭调试模式
0063	脚本执行周期	4	整数	0	脚本定期执行的周期时间，单位为秒，0 表示不周期执行脚本
0064	脚本内容	0-399	字符串	空	DTU 周期执行的脚本，用于自动采集用户仪表数据，详细编写规则请参考脚本手册
0053	HTTP 协议开关	1	0: 关 1: 开	0	在 TCP Client 模式下，如果设置此参数为开，则 DTU 的数据通过 HTTP 协议发送至 WEB 平台，这个功能和脚本功能可以使用户使用众山 DTU 直接采集仪表数据进入 WEB 平台，并且所有控制协议都能在 HTTP 协议中支持，详细的资料请参考众山 DTU HTTP 使用手册
0054	HTTP 方法	1	0: POST 1: GET	0	上传数据使用 POST 或 GET 方法
0058	HTTP 输出头信息	1	0: 不输出 1: 输出	0	在 HTTP 下行数据时，1 表示输出全部的 HTTP 包到串口 0 表示 DTU 解析<data></data>中的有效数据输出到串口
005A	HTTP 长连接短连接设置	1	0: 短连接 1: 长连接	0	在短连接模式下，DTU 被断开连接时不会继续连接中心，直到有上行数据时才会主动连接在长连接模式下，如果连接断开，DTU 会不断尝试连接中心



0055	URL	0-99	字符串	空	HTTP 发送的 URL 地址
0056	HOST	0-99	字符串	空	HTTP 发送的主机地址和端口，格式为 ip:port 或 domain:port
0057	其他头信息	0-99	字符串	空	HTTP 的其他头信息，如果有 多行头信息，请用\r\n 分开， 最后一行不能有\r\n
0059	发送 KEY	0-63	字符串	data	发送数据时使用 KEY=VALUE 的格式，这里定义 KEY 的 值，不同的 DTU 使用不同的 KEY 值可以让 WEB 平台区分 不同的 DTU 或者不同的数 据，为空时 DTU 默认使用 data HTTP 下行数据使用<data>数 据</data>的固定格式，便于 DTU 解析 WEB 下传的真实数 据

注：参数设置成功 DTU 返回 00F0 命令，设置失败或者不支持的参数 DTU 返回 00F1

命令	名称	数据长度
00F0	正确	0
00F1	错误	0

## 2.3 命令详解

### 2.3.1 读取参数

方向	命令	名称	数据	备注
用户设备或 中心到 DTU	E000	读取参数	CMD1 CMD2.....CMDn 每个参数号占 2 个字 节，表示需要读取的 参数，可以一次读多 个参数	建议一次不要读取太多的参数，当 参数值比较长时，多个参数值可能 会超过最大发送量
DTU 响应	E000	响应读取参数 命令	LENG1 CMD1 DATA1 LENG2 CMD2 DATA2 ..... LENGn CMDn	每个参数值以 2 字节长度+2 字节参 数号+参数值的格式应答 2 字节长度包含参数号和参数值的长 度，多个参数返回时按照这样的格 式依次放置

			DATA <sub>n</sub>	
--	--	--	-------------------	--

### 2.3.2 查询 DTU 状态

方向	命令	名称	数据	备注
用户设备或中心到 DTU	E004	查询 DTU 状态	空	
DTU 响应	E004	返回 DTU 状态	1 字节状态	0: DTU 模块关机状态 1: 未注册状态 2: 待机状态 3: PPP 拨号状态 4: 拨号成功, 未连接到中心 5: 连接中心成功

### 2.3.3 参数恢复出厂默认配置

方向	命令	名称	数据	备注
用户设备或中心到 DTU	E003	DTU 参数恢复出厂默认	空	
DTU 响应	00F0	正确	空	

### 2.3.4 查询 DTU 软件版本号

方向	命令	名称	数据	备注
用户设备或中心到 DTU	E001	查询 DTU 软件版本号	空	
DTU 响应	E001	返回版本号	版本号	字符串格式的版本号

### 2.3.5 复位 DTU

方向	命令	名称	数据	备注
用户设备或中心到 DTU	E006	复位 DTU	空	本地复位时, DTU 响应命令 1 秒后复位 远程复位时, DTU 收到命令号响应, 10 秒后复位, 如果网络异常, 有可能出现收不到响应
DTU 响应	00F0	正确	空	

### 2.3.6 查询 DTU IP 地址

方向	命令	名称	数据	备注
----	----	----	----	----

用户设备或中心到 DTU	E007	查询 DTU IP 地址	空	
DTU 响应	E007	返回 IP 地址	4 字节 IP 地址	如 IP 为 10.0.0.1 返回数据为 0A000001

### 2.3.7 查询信号强度

方向	命令	名称	数据	备注
用户设备或中心到 DTU	E023	查询 DTU 信号强度	空	
DTU 响应	E023	返回信号强度	1 字节信号强度	0-31, 数值越大信号越强 99, 无信号

### 2.3.8 查询 IMSI 号码

方向	命令	名称	数据	备注
用户设备或中心到 DTU	E024	查询 IMSI 号码	空	
DTU 响应	E024 或 00F1	返回号码或错误	有号码时返回号码 为空时返回 00F1	当未能读出号码返回 00F1

### 2.3.9 查询 IMEI 号

方向	命令	名称	数据	备注
用户设备或中心到 DTU	E025	查询 IMEI 号码	空	
DTU 响应	E025 或 00F1	返回号码或错误	有号码时返回号码 为空时返回 00F1	当未能读出号码时, 返回 00F1

### 2.3.10 查询 ICCID 号码

方向	命令	名称	数据	备注
用户设备或中心到 DTU	E029	查询 ICCID 号码	空	
DTU 响应	E029 或 00F1	返回号码或错误	有号码时返回号码 为空时返回 00F1	当未能读出号码时, 返回 00F1

### 2.3.11 查询 2/3/4G 和网络服务商

方向	命令	名称	数据	备注
用户设备或中心到 DTU	E027	查询 2/3/4G 状态和网络运营商	空	

DTU 响应	E027	返回号码 2/3/4G 状态和	2G(3G)(4G) (Noservice) (Unknown) China Mobile	2G: 表示注册到 2G 网络 3G: 表示注册到 3G 网络 4G: 表示注册到 4G 网络 No service: 未注册到网络 Unknown: 未知
		网络运营商或 错误	(China Unicom) (China Telecom) (Register Fail) (Unknown)	China Mobile: 中国移动 China Unicom: 中国联通 China Telecom: 中国电信 Register Fail: 注册失败

### 2.3.12 启动脚本执行

方向	命令	名称	数据	备注
用户设备或 中心到 DTU	E026	立即启动本地 脚本执行	空	
DTU 响应	00F0 或 00F1	正确或错误	空	当脚本正在执行时返回错误, 否则 返回正确并且立即启动脚本执行

### 2.3.13 发送数据

方向	命令	名称	数据	备注
用户设备或 中心到 DTU	E020	发送数据	0x0000+数据	用户不仅可以通过串口发送透明数 据外, 也可以通过此命令发送数 据, 数据前的 0x0000 为保留位置, 必须为 0x0000。通过此命令发送数 据的好处是当 DTU 串口缓存满时, DTU 会返回错误, 便于用户掌握发 送数据的进度
DTU 响应	00F0 或 00F1	正确或错误	空	当串口缓存满时返回 00F1, 否则返 回 00F0