



# ZSLxxx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LoRa DTU产品。

本手册主要介绍众山 ZSLxxx、ZSLRxxx 系列 LoRa DTU 串口及远程控制协议。

适用型号：ZSL210、ZSL310、ZSL311、ZSLR311。

## 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：ZSLxxx串口及远程控制协议

版本：1.01

修改日期：2018年12月21日

## 相关文档

- 1、《众山 DTU Modbus 协议手册》
- 2、《众山 DTU 脚本编程手册》

## 一、手册说明

本手册详细描述众山 LoRa DTU 的参数配置细节和各种控制命令，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，而且使用相同的协议通过再封装一层双方网络 ID 的协议可以对对端 LoRa DTU 进行同样的配置和控制。LoRa DTU 在串口端接收到用户数据和接收到对端 LoRa 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，并不透传到对端 LoRa，否则 DTU 会作为透传数据发送到对端 LoRa。DTU 在收到对端 LoRa 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，便于用户在 LoRa 网关端远程控制 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，而是执行相应的 Modbus 指令。当 LoRa DTU 收到对端 LoRa 下发的 Modbus 协议且地址和自己的 Modbus 地址一致时，DTU 会自动回复 Modbus 响应给对端 LoRa，以实现通过远程 LoRa 网关控制多个节点 LoRa 的 DI/DO 功能。

本手册规定的协议在 DTU 串口层和 LoRa 层通用。LoRa 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。如果用户需要在自己的设备中嵌入这些功能，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，还可以从对端 LoRa 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对端 LoRa 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 本地控制协议格式

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

## 2.2 控制对端 LoRa 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 字节开始到最后校验所有的字节数
4	Length_L	长度低字节	
5	73	控制对端 LoRa 命令高字节	固定为 7301，表示通过接下来 2 字节的节点 ID 控制对应 LoRa
6	01	控制对端 LoRa 命令低字节	
7	OBJNode_H	对端 LoRa 节点 ID 高字节	节点 ID 为此的 LoRa DTU 会执行命令且响应执行结果，在 LoRa 响应命令时会和 SRCNode 交换
8	OBJNode_L	对端 LoRa 节点 ID 低字节	
9	SRCNode_H	固定为 FFFF	不能为网络中存在的节点 ID，所以使用 FFFF，在 LoRa 响应命令时会和 OBJNode 交换
10	SRCNode_L		
11	Cmd_H	命令高字节	后面详细解释各种不同的命令
12	Cmd_L	命令低字节	

13~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 2.2

- 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

### 2.3 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
0801	LoRa 频率	4	整数	433000000	LoRa 通讯频率，单位为 Hz。同一网络内的设备频率必须一致
0802	LoRa 发射功率	1	整数	20	LoRa 发射功率，0-20 dbm，功率越大距离越远，发射功耗越高
0F12	LoRa 通讯距离	1	0:空旷 3 公里 3:空旷 6 公里 5:空旷 8 公里	3	通讯距离越远的模式通讯速率越低，数据发送时间越长，延迟越大，功耗越高，此参数定义不同的 LoRa 扩散因子，所以同一网络内的所有 LoRa 必须一致
0F13	LoRa 工作模式	1	0:空中唤醒模式 1:实时发送接收模式 2:纯发送模式 3:发送完限时接收模式	0	为了满足不同应用对功耗的要求，众山 LoRa DTU 提供 4 种工作模式供用户选择 0: 空中唤醒模式 此模式，LoRa DTU 以定时唤醒开启接收的方式工作，此模式可以随时收发数据，但由于采用了空中唤醒技术，所以

					<p>数据延迟最大，功耗较低，适用于用户对功耗要求较高但对数据实时性要求不高的场合 （注意：此模式下要求一个网络内的所有 LoRa DTU 都使用此模式，否则会导致数据异常）</p> <p>1: 实时发送接收模式 此模式，LoRa DTU 发送完后一直开启接收模式，所以可以实时收发数据，但是功耗最大，数据延迟最低，此模式可以和模式 2 和模式 3 混合使用，一般用作 LoRa 网关可以实时接收 LoRa 节点数据</p> <p>2: 纯发送模式 此模式，LoRa DTU 发送完数据后立即关闭接收进入休眠模式直到有串口数据需要发送时，所以此模式功耗极低，适用于只需要发送数据的 LoRa 节点，由于此模式不能接收数据，所以不能使用具有应答机制的 LoRa-TCP 协议。</p> <p>3: 发送完限时接收模式 此模式，LoRa DTU 发完数据后开启一段时间的接收状态，此时间可配置，适用于主动发送数据但又需要发送数据后接收网关数据的应用，在发送数据频次不高的场合，由于开启的接收时间比较短，功耗也比较低。接收时间通过参数可自由配置，当有数据通讯时时间会重置时间，时间到后 LoRa 立即进入休眠。</p>
0F15	LoRa 协议选择	1	0: LoRa-UDP 1: LoRa-TCP	0	<p>为了满足用户对 LoRa 通讯数据可靠性的要求，众山 LoRa DTU 开发了两种通讯机制</p> <p>LoRa-UDP: 不保证数据的可靠性，发送数据后没有底层应答</p>

					<p>LoRa-TCP: 保证数据的可靠性, 数据发送后需要对方应答, 不应答时 LoRa DTU 会重发, 重发次数和超时重发时间可配置, 并且为了防止多个设备同时重发的碰撞问题, 采用了指数退避的方式逐渐增加时间。此模式的重发和应答机制是 LoRa DTU 底层自动完成的, 不需要用户干预, 并且此机制只针对有单一目标地址的数据包, 目标地址为广播或组播的数据包 LoRa DTU 按不应答不重发的机制处理。由于此模式增加了应答机制, 当然数据的发送频率就会变慢。在同一网络中使用相同的协议才能保证重发应答机制工作正常。</p>
0F04	LoRa-TCP 重发开始时间	1	整数	10	<p>在 LoRa-TCP 协议, 当目标 LoRa 设备没有应答数据包, 超过重发开始时间时, LoRa DTU 重发数据包, 以后按照指数退避方法决定下次重发的时间, 重发开始时间单位为秒。重发次数由 0F05 参数决定, 设置的次数到了后仍未应答, 则丢弃该数据包。</p>
0F05	LoRa-TCP 重发次数	1	整数	3	
0F14	限时接收时间	4	整数	30	<p>此参数在 0F13 参数 LoRa 工作模式设置为 3:发送完限时接收模式时才有效, 规定设备在无数据通讯时进入休眠的时间, 单位为秒</p>
08E9	中继模式	1	0: 节点模式 1: 中继模式	0	<p>众山 LoRa DTU 为了适用更长距离通讯或者当设备间遮挡较</p>

			2: 自适应中继模式		严重不能通讯时的情况，采用中继的方式使数据能够在中继站转发数据。节点模式使设备不具有中继功能，中继模式使设备当成纯中继使用，只转发数据不处理数据，自适应中继模式使设备除了能透传自己的数据包时，还能转发不仅仅是自己的数据包。当不需要中继时建议用户不要设置中继功能，否则会造成正常通讯时数据包较多，影响通讯的实时性。
0820	串口波特率	4-6	字符串	“9600”	支持 1200-38400 的波特率
0821	串口配置	3	字符串	“8N1”	配置串口数据位、校验位、停止位，支持 7 位或 8 位数据位，无校验、奇校验、偶校验，支持 1 位或 2 位停止位
0822	串口分包数据间隔时间	2	10-10000	10	串口数据超过时间间隔，DTU 会打包发送，单位为 1 毫秒，即可设置 10 毫秒~10 秒
0052	Modbus 地址	1	整数	100	在有 DI/DO 功能的 DTU 中，用于 DI/DO 控制的 Modbus 地

					址
08EB	发送数据头	0-16	1 字节长度+内容	0	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。此参数便于用户使用配置不同的头区分不同的 DTU
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	0-199	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
0824	网络 ID	4	整数	1	通过网络 ID 和网络密码参数可以把频率相同的 LoRa 分成不同的逻辑网络，只有网络 ID 和密码相同的 DTU 才能进行数据通讯
0826	网络密码	2	整数	23190	
0825	节点 ID	2	整数	1	一个网络内每个 LoRa DTU 配置不同的节点 ID，可以实现指向目标 ID 的点对点通讯
0827	目标节点 ID	2	整数	65535	设置数据发送的目标 ID，设置为需要接收数据包的 LoRa DTU 的节点 ID，当节点 ID 与此目标节点 ID 不一致的 LoRa 不会处理此数据包。设置为 FFFF(65535)为广播发送，同一逻辑网络内所有 LoRa 都可以选择接收到广播包
0F11	组播 ID	2	整数	65534	为了能在同一逻辑网络内可以进行分组通讯，众山 LoRa DTU 支持组播通讯，当组播地址一样的 DTU 可以接收到目标节点 ID 为与自己组播 ID 相同的数据包。组播发送时只需要把目标节点 ID 设置为对方的组播 ID
0F10	接收 ID 模式	1	0:接收 ID 为自己和广播包 1:接收 ID 为自己和组播包 2:只接收 ID 为自己的包	3	此参数可以配置 LoRa DTU 有选择性的接收数据，可以配置接不接收广播包、组播包等。

			3:接收自己、广播和组播包 4:不限 ID, 接收所有包		
--	--	--	---------------------------------	--	--

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
串口到 DTU	7000	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	F000	响应读取参数命令	LENG1 CMD1 DATA1 LENG2 CMD2 DATA2 ..... LENGn CMDn DATA n	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

### 2.3.2 参数恢复出厂默认配置

方向	命令	名称	数据	备注
串口到 DTU	7003	DTU 参数恢复出厂默认	空	
DTU 响应	00F0	正确	空	

### 2.3.3 查询 DTU 软件版本号

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

串口到 DTU	7001	查询 DTU 软件版本号	空	
DTU 响应	F001	返回版本号	版本号	字符串格式的版本号

### 2.3.4 复位 DTU

方向	命令	名称	数据	备注
串口到 DTU	7006	复位 DTU	空	
DTU 响应	00F0	正确	空	

### 2.3.5 查询电池电压

方向	命令	名称	数据	备注
串口到 DTU	7202	查询电池电压	空	
DTU 响应	F202	返回电池电压	2 字节的电池电压， 除以 100，得到实际的电压值	如 2 字节的电池电压值为 330，则表示电池电压为 3.3V

### 2.3.6 查询 RSSI 信号强度

方向	命令	名称	数据	备注
串口到 DTU	7206	查询 RSSI 信号强度	空	
DTU 响应	F206	返回信号强度	2 字节的节点 ID+1 字节信号强度	节点 ID: 表示和 LoRa 最近一次通讯的 LoRa DTU 的节点 ID 信号强度: 0-100, 数值越大信号越强

### 2.3.7 启动脚本执行

方向	命令	名称	数据	备注
串口到 DTU	720A	立即启动本地脚本执行	空	
DTU 响应	00F0 或	正确或错误	空	当脚本正在执行时返回错误，否则

	00F1			返回正确并且立即启动脚本执行
--	------	--	--	----------------

### 2.3.8 发送数据

方向	命令	名称	数据	备注
串口到 DTU	7200	发送数据	2 字节目标节点 ID+数据	用户不仅可以通过串口发送透明数据，也可以通过此命令发送数据。通过此命令发送数据的好处是在协议中指定此次发送的目标节点 ID，当 2 字节的目标节点 ID 为 0000 时表示使用 DTU 参数中配置的目标节点 ID，不为 0000 时表示使用协议指定的目标节点 ID。当发送的数据超过 210 字节时，DTU 会返回错误
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