ZSNxx1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NB-IoT DTU产品。

本手册主要介绍众山 ZSNxx1、ZSNRxx1 系列 NB-IoT DTU 远程控制协议。

适用型号：ZSN211、ZSN311、ZSN221、ZSN321、ZSNR311、ZSNR311。

版权声明

版本信息

文档名称：ZSNxx1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、《ZSNxx1 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
3、增加 E00C 命令读取电池电压

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，UDP Master/UDP-ZSD/CoAP。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数
4	Length_L	长度低字节	
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 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 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” “ctnb”	这些参数用于 DTU 在接入不同专网时使用。 电信版默认 ctnb 移动版默认 CMNET
0033	接入点用户名			“WAP”	
0034	接入点密码			“WAP”	
0035	主 DNS IP 地址	4	HEX	电信版 DA040404 移动版 D388116B	在中心使用域名的情况下需要使用,电信版默认 218.4.4.4 和 218.2.2.2 。移动版默认 211.136.17.107 和 211.136.20.203
0036	副 DNS IP 地址			电信版 DA020202 移动版 D38814CB	
0045	串口波特率	4-9	字符串	“9600”	支持 1200-38400 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 NB-IoT 模组，用户用 AT 命令自己开发所有功能
0040	网络模式	1	1：UDP-ZSD 3:UDP Master 10:CoAP	0	UDP-ZSD 为众山 DTU 在 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，UDP Master 模式为全透明 UDP，在此模式下用户可以自定义登录心跳等，也可以不配置，CoAP 协议为基于 UDP 的物联网协议，当要连接 CoAP 平台时（如电信物联云平台）时使用此协议
0041	中心 IP 地址或域名	0-31	字符串	空	中心的 IP 地址或者域名
0042	中心端口	0-5	字符串	空	中心的端口
0100	CoAP 平台地址	0-31	字符串	180.101.147.115	CoAP 平台的地址和端口
0101	CoAP 平台端口	0-5	字符串	5683	
0044	心跳时间	2	整数	30 小时	心跳时间，在 NB-IoT DTU,为了让 2 字节的心跳时间参数能表示更长的时间，采用最高位(bit15)为 1 时，单位为分钟，最高位为 0 时单位为秒，bit15 不参与时间的计算，只表示单位。默认 0x8708，最高位为 1，单位为分钟，表示 0x0708 分钟，即 30 小时。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，	0	规定在 UDP Master 和 CoAP 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

			需要中心应答		送几次仍未应答时 DTU 进入重连状态
004A	心跳包发送内容	0-31	1 字节长度+内容	0	UDP Master 和 CoAP 模式下的心跳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
004B	心跳包应答内容				
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 UDP Master 和 CoAP 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	UDP Master 和 CoAP 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	UDP Master 和 CoAP 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
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	物联云登录密码	6	字符串	“000000”	登录众山物联云密码

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

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 DATAn	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 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: 开始创建 SOCKET 状态 4：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

2.3.7 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

2.3.8 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

2.3.9 查询 SIM 卡的 ICCID 号

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

2.3.10 查询电池电压

方向	命令	名称	数据	备注
用户设备或中心到 DTU	E00C	查询电池电压	空	
DTU 响应	00F0	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

2.3.11 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

2.3.12 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。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