
物联网电力线载波模块

M220N

用户手册

V1.0

上海中基国威电子股份有限公司
SHANGHAI SINOMICON ELECTRONICS CO., LTD

2019 年 03 月 04 日



第1章

目 录

第 1 章 模块简介.....	4
1.1 技术参数	4
1.2 模块接口定义.....	4
1.3 状态指示灯.....	5
第 2 章 数据通信.....	7
2.1 MCU 通信接口.....	7
2.2 模块通讯流程.....	7
第 3 章 报文基本格式.....	8
3.1 报文格式	8
3.2 FN 的类型	8
第 4 章 接口协议.....	9
4.1 MCU 设置模块 MAC 地址(FE 01).....	9
4.2 查询 MAC 地址(FC 01).....	9
4.3 回复 MAC 地址(FD 01)	9
4.4 查询节点状态信息(FC 06).....	10
4.5 回复节点状态信息(FD 06)	10
4.6 CCO 模块启动组网(FE 0D).....	11
4.7 CCO 模块结束组网(FE 0E)	11
4.8 STA 查找可用网络(FC 09)	11
4.9 STA 回复可用网络(FD 09).....	12
4.10 STA 加入网络(FE 03).....	12
4.11 STA 离开网络(FE 04).....	13
4.12 模块入网指示(FE 09)	13
4.13 设置重启模块(FE 12)	13
4.14 模块离网指示(FE 0A)	14
4.15 模块启动提示(FE 18)	14
4.16 模块发 BEACON 提示(FE 15).....	15
4.17 MCU 设置白名单(FE 05).....	15
4.18 MCU 查询白名单(FC 07).....	15
4.19 模块回复白名单(FD 07)	16
4.20 确认帧格式(FE 14)	16
4.21 MCU 数据传输命令(FE A0).....	17
4.22 MCU 设置模块串口波特率(FE A1).....	17
4.23 MCU 查询模块串口波特率(FC 0E).....	18
4.24 模块返回串口波特率索引(FD 0E)	18
4.25 扩展命令查询白名单(FC 0F)	19
4.26 扩展命令查询白名单查询结果上报(FD 0F)	19
4.27 MCU 设置网络 ID(FE 11)	19
4.28 MCU 查询网络 ID(FC 10)	20
4.29 模块回复网络 ID(FD 10).....	20
4.30 MCU 设置工作频段(FE 1C).....	21
4.31 MCU 设置扫描频段(FE 1E)	21
4.32 MCU 查询扫描频段(FC 14).....	21
4.33 模块回复扫描频段(FD 14).....	23
4.34 MCU 查询模块信息(FC 12).....	23
4.35 模块回复本地基本信息(FD 12)	23
4.36 查询白名单状态(FC 11).....	24
4.37 回复白名单状态(FD 11)	s24
4.38 设置发射功率(FE 16)	24



4.39 查询发射功率(FC 0B)	25
4.40 回复发射功率(FD 0B)	25
4.41 查询 CCO 工作频段(FC 16)	25
4.42 回复 CCO 工作频段 (FD 16)	26
4.43 查询节点信息(FC 17)	26
4.44 回复节点信息 (FD 17)	27
第 5 章 CRC16 生成方法	28
第 6 章 附录：常用定义	30
附录 1 设置命令出错原因	30



第1章 模块简介

物联网电力线载波模块 M220N 是一款由上海中基国威电子股份有限公司自主研发的适用于低压电力线载波通讯的产品。其核心部分主控制芯片基于 OFDM 调制解调技术，克服低压电力线的各种干扰进行高可靠数据传输，具有高速率、抗电力线干扰强的特点。工作频段为 0.7~30MHz。芯片集成了模拟收发通道和物理层通信基带，传输介质为 220V 低压电力线，传输模式为半双工。

该模块外围器件少，可简化整体电路设计，主要用于家电智能控制，路灯控制等领域，为电力行业或其它公共事业部门提供了一种优秀系统解决方案。

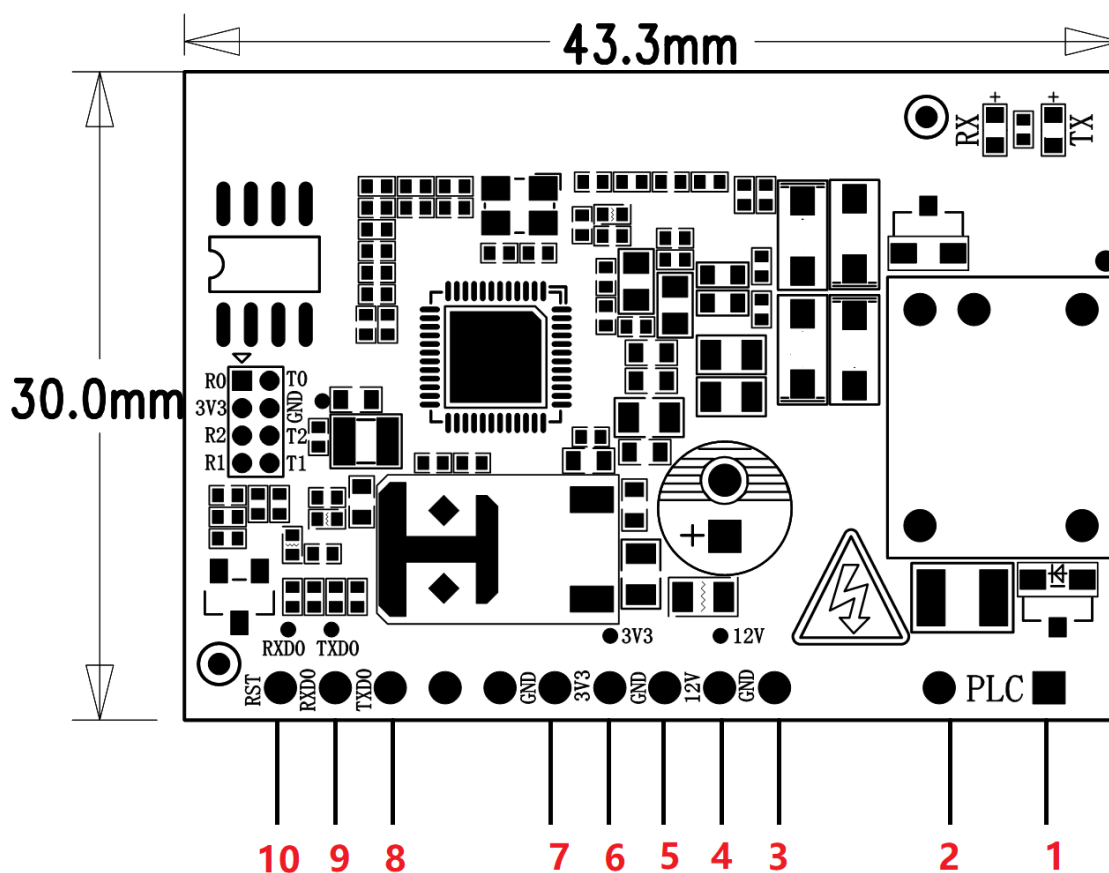
1.1 技术参数

物联网电力线载波模块 M220N 接口模块的主要技术参数如表所示。

工作频段	0.7~34.5MHz
串口通讯速率	2400bps、9600bps、115200bps
工作频率	50Hz/60Hz
静态功耗	≤0.4W
动态功耗	≤1.5W
工作温度	-40℃~+85℃
相对湿度	≤75%
通讯范围	整个配变台区
抗衰减性能	>115dB
重负载下抗衰减性能	>105dB (1 欧姆负载)
强干扰下抗衰减性	>55dB (20Vpp 3MHz 方波干扰)
最大路由级数及最大子节点量	最大路由级数15 级，最大子节点数900 个，可扩充至1014 个节点
工作可选频段	band0: 2M~12Mhz band1: 2.5M~5.6Mhz band2: 700k~3Mhz band3: 1.7M~3Mhz band4: 5.6M~12Mhz band8: 5.8M~9Mhz band9: 4.9M~24.4Mhz band10: 28.3M~34.5Mhz band11: 4.9M~12.2Mhz

1.2 模块接口定义

物联网电力线载波模块 M220N 模块尺寸为 43.3mm*30mm;



M220N 接口采用 2.54mm 间距插针设计，接口管脚定义为：

编号	接口名称	信号类别	说明
1	L_PLC	信号	电网 L 线作为信号耦合接入端，对应终端底板需要串联 10nF 安规电容
2	N_PLC	信号	电网 N 线作为信号耦合接入端，对应终端底板需要串联 10nF 安规电容
3	GND	电源地	电源地
4	12V	12V 电源正极	直流电压范围 $12V \pm 1V$ ，电源纹波不大于 120mV，输出电流不小于 200mA。需接 100uF/25V 以上电解电容
5	GND	电源地	电源地
6	3V3	3.3V 电源正极	3.3V \pm 0.3V 信号电源，电流 150mA，纹波 5% 以内
7	GND	电源地	电源地
8	TXD0	信号	UART 发射信号（3.3V TTL 电平），与 MCU 进行通讯
9	RXD0	信号	UART 接收信号（3.3V TTL 电平），与 MCU 进行通讯
10	RST	复位信号	复位输出（低电平有效），开漏方式，常态为高阻态，可用于复位通信模块，复位信号脉宽不小于 200ms。无特殊需求可以不接。

1.3 状态指示灯

模块有 2 个贴片 LED 指示灯用于指示状态：红色为 TX 指示灯，黄色为 RX 指示灯。



模块入网前，STA 模块的 TX 指示灯和 RX 指示灯常亮；CCO 模块的 TX 指示灯常亮、RX 指示灯闪烁。
模块入网成功后，STA 模块的 TX 指示灯常亮、RX 指示灯闪烁；CCO 模块的 TX 指示灯常亮、RX 指示灯闪烁。

SINOMICON



第2章 数据通信

MCU 和模块之间通信的物理接口是 UART，MCU 和模块各自维护 UART 驱动。

默认通信参数为：115200bit/s、8 数据位、1 停止位、无校验，可根据协议修改波特率。

2.1 MCU 通信接口

MCU 通过 UART 将数据传输到模块，模块通过 PLC 将数据转发到 target 网络节点，target 网络节点收到 PLC 上的数据后，通过 UART 将数据上报给 MCU。

MCU 控制软件通信流程：

- 1、初始上电，模块会自动发出启动提示（FE 18），MCU 读到模块启动提示后，查询模块信息（FC 12），读取模块返回信息（FD 12），可根据信息读出 mac 地址和模块角色，确定该模块是 CCO 还是 STA；
- 2、模块组网：
 - （1）通过 CCO 端添加白名单的方式组网：STA 模块白名单功能禁用（FE 05），在 CCO 的白名单内加入对应的模块地址（FE 05）；STA 模块会选择信道质量优的 CCO 网络自动组网（入网时间 20s~40s）；
 - （2）通过 CCO 端开启组网方式组网：STA 模块白名单功能使能（FE 05），CCO 模块启动组网（FE 0D），STA 模块不断查询可用网络（FC 09），根据回复的信息（FD 09），选择加入网络（FE 03）；入网时间根据当前 snr 的大小确定；
 - （3）入网成功后，模块会返回入网成功信息（FE 09）；
- 3、在 PLC-STA 模块提示入网后，才开始进行数据传输；
- 4、在 PLC-STA 模块提示离网后，停止数据传输；
- 5、在 PLC-CCO 模块收到 STA 加入提示后，才开始数据传输；
- 6、在 PLC-CCO 模块发现没有 STA 加入时，停止数据传；
- 7、尽量避免在 PLC 网络里传输冗余信息。

安装注意事项

- 1、请勿掰动模块上的安规电容等器件，避免人为损坏。
- 2、由于模块上有高压线路，请勿在不安装外壳的情况下将模块插拔，以免造成人身伤害。
- 3、请勿过度用力按压模块。

2.2 模块通讯流程

1. 系统上电后，CCO 模块或者 STA 模块首先会向 MCU 请求 MAC 地址。
2. 如果超时后 MCU 不应答，通信模块会继续请求，MCU 设置了 MAC 地址后 CCO 模块会开始发信标数据，STA 模块会进入入网流程。
3. 通讯模块入网：模块入网有两种方式。
 - 1) 通过 CCO 端添加白名单的方式组网：在 CCO 端的白名单内加入对应的模块地址，在模块端需要将白名单功能禁用，设置完成后 STA 模块会选择信道质量优的 CCO 网络加入。
 - 2) 通过 CCO 端开启组网的方式组网：CCO 端进入组网模式，STA 模块使能白名单后通过查找 CCO 网络，再加入 CCO 网络。
4. 通讯模块的数据收发：MCU 通过数据帧格式可实现数据的单播、广播传输。



第3章 报文基本格式

3.1 报文格式

0xAA 0xAA LEN FN SUBFN RESV[0] RESC[1] PAYLOAD CRC0~7 CRC8~15 0xFF 各字段含义如下表:

字段	字节数(Byte)	含义
LEN	1	payload 域字节长度
FN	1	主功能码
SUBFN	1	子功能码
RESV[0]	1	保留 (部分协议中会用到)
RESV[1]	1	保留 (部分协议中会用到)
PAYLOAD	LEN (0~255)	MCU 数据报文
CRC 0~16	2	16 位CRC, 计算生成方法后附。范围从0xAA AA 开始, 到 PAYLOAD 结尾。

3.2 FN 的类型

FN 类型如下表所示:

FN	含义
0xFC	query, 查询功能码
0xFD	response, 回复功能码
0xFE	set, 设置功能码



第4章 接口协议

MCU 对模块的 set 命令都需要有确认帧 confirm, query 命令都要有 response 回复。模块主动上报的指示命令（归于 set 命令），不需要 MCU 回复确认帧。

4.1 MCU 设置模块 MAC 地址(FE 01)

MCU 设置本地 MAC:

0xAA 0xAA 0x07 0xFE 0x01 0x00 0x00 SEQ MAC0~5 SUM 0xFF

字段	含义
0xAA 0xAA	Preamble
0x07	Payload 长度
0xFE	功能码
0x01	MAC 地址设置子功能码
0x00	Resv0
0x00	Resv1
SEQ	报文序列号
MAC0~5	MAC 地址
SUM	CRC16
0xFF	Tail code

模块收到所有的 SET 设置命令后，均会回复响应确认。确认报文 CMD_CONFIRM 的格式在后面会描述。

4.2 查询 MAC 地址(FC 01)

MCU 查询本地模块 MAC:

0xAA 0xAA 0x03 0xFC 0x01 0x00 0x00 SEQ DIR ROLE SUM 0xFF

字段	含义
0xAA 0xAA	Preamble
0x03	Payload 长度
0xFC	功能码
0x01	MAC 地址查询子功能码
0x00	Resv0
0x00	Resv1
SEQ	报文序列号 (MCU 维护, 递增)
DIR	为0 表示查询模块MAC 地址, 为1 时, 表示查询MCU MAC
ROLE	网络角色, 填0 即可
SUM	CRC16
0xFF	Tail code

4.3 回复 MAC 地址(FD 01)

0xAA 0xAA 0x09 0xFD 0x01 0x00 0x00 SEQ DIR MAC0~5 NW_ROLE SUM 0xFF



字段	含义
0xAA 0xAA	Preamble
0x09	Payload 长度
0xFD	功能码
0x01	MAC 地址回复子功能码
0x00	Resv0
0x00	Resv1
SEQ	报文序列号 (MCU 维护, 递增)
DIR	为0, 表示回复模块的MAC 地址, 为1 时, 表示回复MCU MAC
MAC0~5	回复的MAC 地址
NW_ROLE	网络角色: 1--STA, 2--PCO, 4--CCO
SUM	CRC16
0xFF	Tail code

4.4 查询节点状态信息(FC 06)

0xAA 0xAA 0x07 0xFC 0x06 0x00 0x00 SEQ MAC0~5 SUM FF

字段	含义
0xAA 0xAA	Preamble
0x07	Payload 长度
0xFC	功能码
0x06	查询节点状态信息子功能码
0x00	Resv1
0x00	Resv2
SEQ	报文序列号 (模块维护, 递增)
MAC0~5	查询及节点状态信息, FF:FF:FF:FF:FF:FF 为查询全网所有STA 节点的状态信息, 00:00:00:00:00:00 为查询当前节点状态信息。
SUM	CRC16
0xFF	Tail code

4.5 回复节点状态信息(FD 06)

0xAA 0xAA 0x0D 0xFD 0x06 SNR NF SEQ TOTAL_L TOTAL_H CUR_L CUR_H MAC0~5 SUM FF

字段	含义
0xAA 0xAA	Preamble
0x0D	Payload 长度
0xFD	功能码
0x06	回复节点状态信息子功能码



SNR	信噪比
NF	底噪
SEQ	报文序列号（模块维护，递增）
TOTAL_x	总共回复的信息条数，TOTAL_H—16 位数据高8 位，TOTAL_L—16 位数据低8 位
CUR_x	当前信息编号，CUR_H—16 位数据高8 位，CUR_L—16 位数据低8 位
MACO~5	回复节点对应的MAC 地址
SUM	CRC16
0xFF	Tail code

4.6 CCO 模块启动组网(FE 0D)

CCO 模块启动组网，以方便其他STA 加入到该网络。

0xAA 0xAA 0x07 0xFE 0x0D NID 0x00 SEQ MACO~5 SUM 0xFF

字段	含义
0xAA 0xAA	Preamble
0x07	Payload 长度
0xFE	功能码
0x0D	设置启动组网子功能码
NID	网络标识
0x00	Resv1
SEQ	报文序列号（MCU 维护，递增）
MACO~5	6 字节CCO 模块MAC 地址
SUM	CRC16
0xFF	Tail code

4.7 CCO 模块结束组网(FE 0E)

CCO 启动组网后，等待需要的STA 入网后可以发送结束组网命令。其他未加入的STA 再申请加入时，CCO 将拒绝其加入网络。

0xAA 0xAA 0x07 0xFE 0x0E NID 0x00 SEQ MACO~5 SUM 0xFF

字段	含义
0xAA 0xAA	Preamble
0x07	Payload 长度
0xFE	功能码
0x0E	设置结束组网子功能码
NID	网络标识
0x00	Resv1
SEQ	报文序列号（MCU 维护，递增）
MACO~5	6 字节CCO 模块MAC 地址
SUM	CRC16
0xFF	Tail code

4.8 STA 查找可用网络(FC 09)



0xAA 0xAA 0x01 0xFC 0x09 0x00 0x00 SEQ SUM FF

字段	含义
0xAA 0xAA	Preamble
0x01	Payload 长度
0xFC	功能码
0x09	STA 查找可用网络子功能码
0x00	Resv1
0x00	Resv2
SEQ	报文序列号 (模块维护, 递增)
SUM	CRC16
0xFF	Tail code

4.9 STA 回复可用网络(FD 09)

0xAA 0xAA 0x01 0xFD 0x09 0x00 0x00 SEQ TOTAL CNT CUR CNT NIDO MAC0-5 NIDn MAC0-5
SUM 0xFF

字段	含义
0xAA 0xAA	Preamble
0x01	Payload 长度
0xFD	功能码
0x09	STA 回复可用网络子功能码
0x00	Resv1
0x00	Resv2
SEQ	报文序列号 (模块维护, 递增)
TOTAL CNT	可用网络总的数量
CUR CNT	当前报文包含的数量
NIDO	第一个可用网络的网络标识
MAC0-5	第一个可用网络 CCO 的 MAC 地址口
.....	
NIDn	第 n 个可用网络的网络标识
MAC0-5	第 n 个可用网络 CCO 的 MAC 地址
SUM	CRC16
0xFF	Tail code

4.10 STA 加入网络(FE 03)

0xAA 0xAA 0x01 0xFE 0x03 NID 0x00 SEQ SUM FF

字段	含义
0xAA 0xAA	Preamble
0x01	Payload 长度
0xFE	功能码
0x03	STA 加入网络子功能码
NID	网络标识
0x00	Resv1
SEQ	报文序列号 (模块维护, 递增)
SUM	CRC16
0xFF	Tail code

通过查询到可用网络的网络ID 加入到对应的网络。



4.11 STA 离开网络(FE 04)

0xAA 0xAA 0x01 0xFE 0x04 NID 0x00 SEQ SUM FF

字段	含义
0xAA 0xAA	Preamble
0x01	Payload 长度
0xFE	功能码
0x04	STA 离开网络子功能码
NID	网络标识
0x00	Resv1
SEQ	报文序列号（模块维护，递增）
SUM	CRC16
0xFF	Tail code

4.12 模块入网指示(FE 09)

CONNECT_IND (STA 入网提示), CCO 方有STA 入网, 会上报MCU 入网指示; STA 入网, 会上报 MCU 入网指示。

0xAA 0xAA 0x09 0xFE 0x09 NID 0x00 SEQ MAC0~5 RSSI SNR SUM 0xFF

字段	含义
0xAA 0xAA	Preamble
0x09	Payload 长度
0xFE	指示功能码, 同设置命令, 模块发给MCU, 不需要MCU 回复
0x09	入网指示子功能码
NID	网络标识
0x00	Resv1
SEQ	报文序列号（模块维护，递增）
MAC0~5	STA 侧, 这里表示CCO MAC 地址; CCO 侧, 这里表示STA MAC 地址
RSSI	信号强度
SNR	信噪比
SUM	CRC16
0xFF	Tail code

4.13 设置重启模块(FE 12)

0xAA 0xAA 0x0D 0xFE 0x12 NID 0x00 SEQ SRC_MAC0~5 DST_MAC0~5 SUM 0xFF

字段	含义
0xAA 0xAA	Preamble
0x0D	Payload 长度
0xFE	功能码
0x12	设置重启模块子功能码
NID	网络标识
0x00	Resv1



SEQ	报文序列号（模块维护，递增）
SRC_MAC0~5	原始MAC 地址
DST_MAC0~5	目的设备MAC 地址
SUM	CRC16
0xFF	Tail code

本地设备收到重启命令，如果目的MAC 地址和本模块一致则会重启本模块，还可以通过网络识别号和对应设备的MAC 地址来重启网络中的其他模块。

4.14 模块离网指示(FE 0A)

DISCONNECT_IND（STA 离网提示），CCO 方有STA 离网，会上报MCU 离网指示；STA 离网，会上报MCU 离网指示。

0xAA 0xAA 0x08 0xFE 0x0A NID 0x00 SEQ MAC0~5 REASON SUM 0xFF

字段	含义
0xAA 0xAA	Preamble
0x08	Payload 长度
0xFE	功能码，同设置命令，模块发给MCU，不需要MCU 回复
0x0A	离网指示子功能码
NID	网络标识
0x00	Resv1
SEQ	报文序列号（模块维护，递增）
MAC0~5	STA 侧，这里表示CCO MAC 地址；CCO 侧，这里表示STA MAC 地址
REASON	离线原因
SUM	CRC16
0xFF	Tail code

4.15 模块启动提示(FE 18)

0xAA 0xAA 0x0D 0xFE 0x18 0x00 0x00 SEQ LOCAL_MAC0~5 CCO_MAC0~5 SUM 0xFF

字段	含义
0xAA 0xAA	Preamble
0x0D	Payload 长度
0xFE	功能码，同设置命令，模块发给MCU，不需要MCU 回复
0x18	模块启动提示子功能码
0x00	Resv1
0x00	Resv2
SEQ	报文序列号（模块维护，递增）
LOCAL_MAC0~5	模块本地MAC 地址
CCO_MAC0~5	CCO MAC 地址
SUM	CRC16
0xFF	Tail code



4.16 模块发 BEACON 提示(FE 15)

0xAA 0xAA 0x03 0xFE 0x15 0x00 0x00 SEQ READY NID SUM 0xFF

字段	含义
0xAA 0xAA	Preamble
0x03	Payload 长度
0xFE	功能码, 同设置命令, 模块发给MCU, 不需要MCU 回复
0x15	CCO 发beacon 提示子功能码
0x00	Resv1
0x00	Resv2
SEQ	报文序列号 (模块维护, 递增)
READY	1: ready 0: not ready
NID	网络标识
SUM	CRC16
0xFF	Tail code

4.17 MCU 设置白名单(FE 05)

CCO 设置完MAC 地址后, 会同时使能白名单, 如果STA 不在CCO 的白名单内, 则不允许入网。只有在CCO 白名单内的STA, 才允许入网。

设置网络白名单。一次设置多个帧时, SEQ 保持不变, TOTOAL 代表帧总数, CUR 为当前帧号。

当CUR=TOTAL 时, 标识本次白名单设置结束, 设置开始生效。

STA 可以开启白名单, 然后自动选择最优网络请求加入。当命令为使能、禁用白名单时, TOTAL 和 CUR 填0。

0xAA 0xAA 0x0B 0xFE 0x05 ACTION 0x00 SEQ TOTAL_L TOTAL_H CUR_L CUR_H MAC0~5 SUM 0xFF

字段	含义
0xAA 0xAA	Preamble
0x0B	Payload 长度
0xFE	功能码
0x05	设置白名单子功能码
ACTION	0: delete mac in whitelist 1: add mac to whitelist 2: disable whitelist
0x00	Resv1
SEQ	报文序列号 (MCU 维护, 递增)
TOTAL_x	本次设置的总的MAC 地址数量, TOTAL _H—16 位数据高8 位, TOTAL _L—16 位数据低8 位
CUR_x	当前mac 地址在总数中的序号, 从1 开始, CUR _H—16 位数据高8 位, CUR _L—16 位数据低8 位
MAC0~5	需要设置到白名单中的MAC
SUM	CRC16
0xFF	Tail code

4.18 MCU 查询白名单(FC 07)

0xAA 0xAA 0x02 0xFC 0x07 0x00 0x00 SEQ CCO_FLAG SUM 0xFF



字段	含义
0xAA 0xAA	Preamble
0x02	Payload 长度
0xFC	功能码
0x07	白名单查询子功能码
0x00	Resv1
0x00	Resv2
SEQ	报文序列号 (MCU 维护, 递增)
CCO_FLAG	0: 查询本地保存的白名单 1: 查询CCO 端的白名单; CCO 端的MCU 查询CCO 的白名单需要此字段写成0
SUM	CRC16
0xFF	Tail code

4.19 模块回复白名单(FD 07)

返回PLC 设备保存的白名单。当TOTAL=CUR 时, 表明所有白名单已经返回。

0xAA 0xAA 0x0B 0xFD 0x07 0x00 CCO_FLAG SEQ TOTAL_L TOTAL_H CUR_L CUR_H MAC0~5 SUM
0xFF

字段	含义
0xAA 0xAA	Preamble
0x0B	Payload 长度
0xFD	功能码
0x07	白名单回复子功能码
0x00	Resv1
CCO_FLAG	0: 本地存储的白名单, 1: CCO 存储的白名单
SEQ	报文序列号 (MCU 维护, 递增)
TOTAL_x	本次设置的总的MAC 地址数量, TOTAL_H—16 位数据高8 位, TOTAL_L—16 位数据低8 位
CUR_x	当前mac 地址在总数中的序号, 从1 开始, CUR_H—16 位数据高8 位, CUR_L—16 位数据低8 位
MAC0~5	返回白名单中的MAC
SUM	CRC16
0xFF	Tail code

4.20 确认帧格式(FE 14)

MCU 命令响应。CMD 为响应的SET 命令, SUBFN 码

RESULT 0 代表成功, 非零代表失败, 失败原因可查询附录1. 设置命令出错原因

0xAA 0xAA 0x03 0xFE 0x14 CMD 0x00 SEQ RESULT REASON SUM 0xFF

字段	含义
0xAA 0xAA	Preamble
0x03	Payload 长度
0xFE	功能码
0x14	确认帧子功能码
CMD	Set 命令的子功能码



0x00	Resv
SEQ	报文序列号 (MCU 维护, 递增)
RESULT	Set 命令执行结果 0: 成功 1: 失败
REASON	RESULT 为1 时有效; 表示set 命令执行失败的原因
SUM	CRC16
0xFF	Tail code

4.21 MCU 数据传输命令(FE A0)

DATA CMD 数据传输, 模块与MCU 之间的数据通路. DSTMAC, 填目标设备ID. 全FF 为广播. 全0 为非法。

0xAA 0xAA LEN 0xFE 0xA0 SENDTYPE DATATYPE DSTMAC0~5 APPDATA SUM 0xFF

字段	含义
0xAA 0xAA	Preamble
LEN	Payload 长度, 不定长
0xFE	功能码
0xA0	数据子功能码
SENDTYPE	Bit0:0--有连接报文, 1--无连接报文, bit1: 0--聚包, 1--不聚包
DATATYPE	0:host data 1:internal beacon data
DSTMAC0~5	目的地址, 全FF 表示广播数据
APPDATA	需要传输的数据帧载荷
SUM	CRC16
0xFF	Tail code

LEN =6+LENGTH(APPDATA)

DATA_LENGTH(APPDATA) < (255-6)

4.22 MCU 设置模块串口波特率(FE A1)

BAUD_ID 值与波特率值对应关系:

BAUD_ID	波特率
0	115200
1	9600
2	2400
3	256000
4	3000000
5-255	无效

0xAA 0xAA 0x02 0xFE 0xA1 0x00 0x00 SEQ BAUD_ID SUM 0xFF



字段	含义
0xAA 0xAA	Preamble
0x02	Payload 长度
0xFE	功能码
0xA1	设置模块波特率子功能码
0x00	Resv1
0x00	Resv2
SEQ	报文序列号 (MCU 维护, 递增)
BAUD_ID	波特率索引
SUM	CRC16
0xFF	Tail code

4.23 MCU 查询模块串口波特率(FC 0E)

0xAA 0xAA 0x01 0xFC 0x0E 0x00 0x00 SEQ SUM 0xFF

字段	含义
0xAA 0xAA	Preamble
0x01	Payload 长度
0xFC	功能码
0x0E	查询模块波特率子功能码
0x00	Resv1
0x00	Resv2
SEQ	报文序列号 (MCU 维护, 递增)
SUM	CRC16
0xFF	Tail code

4.24 模块返回串口波特率索引(FD 0E)

返回查询到的波特率, BAUD_ID 值与波特率值对应关系和设置时一致

0xAA 0xAA 0x02 0xFD 0x0E 0x00 0x00 SEQ BAUD_ID SUM 0xFF

字段	含义
0xAA 0xAA	Preamble
0x02	Payload 长度
0xFD	功能码
0x0E	模块回复波特率子功能码
0x00	Resv1
0x00	Resv2
SEQ	报文序列号 (MCU 维护, 递增)
BAUD_ID	波特率索引
SUM	CRC16
0xFF	Tail code



4.25 扩展命令查询白名单(FC 0F)

0xAA 0xAA 0x05 0xFC 0x0F 0x00 0x00 SEQ START_L START_H CNT_L CNT_H SUM 0xFF

字段	含义
0xAA 0xAA	Preamble
0x05	Payload 长度
0xFC	功能码
0x0F	扩展查询白名单子功能码
0x00	Resv1
0x00	Resv2
SEQ	报文序列号 (MCU 维护, 递增)
START_x	白名单索引, START_H—16 位数据高8 位, START_L—16 位数据低8 位, 表示从第几个开始查询, 最小值是1
CNT_x	CNT_H—16 位数据高8 位, CNT_L—16 位数据低8 位, 表示本次查询多少个STA 的 MAC 地址
SUM	CRC16
0xFF	Tail code

4.26 扩展命令查询白名单查询结果上报(FD 0F)

0xAA 0xAA DATA_LEN 0xFD 0x0F 0x00 0x00 SEQ TOTAL_L TOTAL_H CUR_L CUR_H MAC1 ... MACn SUM 0xFF

字段	含义
0xAA 0xAA	Preamble
DATA_LEN	Payload 长度
0xFD	功能码
0x0F	扩展查询白名单返回子功能码
0x00	Resv1
0x00	Resv2
SEQ	报文序列号 (MCU 维护, 递增)
TOTAL_x	白名单总数量, TOTAL_H—16 位数据高8 位, TOTAL_L—16 位数据低8 位
CUR_x	本次上报数量, CUR_H—16 位数据高8 位, CUR_L—16 位数据低8 位
MAC1~MAC n	假如本次上报个数是5, 这里就是5 个mac 地址, 总共5*6=30byte
SUM	CRC16
0xFF	Tail code

4.27 MCU 设置网络 ID(FE 11)

0xAA 0xAA 0x97 0xFE 0x11 NID 0x00 SEQ MAC0~MAC5 SUM 0xFF

字段	含义
0xAA 0xAA	Preamble
0x97	Payload 长度
0xFE	功能码
0x11	MCU 设置CCO 网络标识子功能码



NID	网络标识
0x00	Resv1
SEQ	报文序列号 (MCU 维护, 递增)
MAC0~MAC5	6 字节CCO 的MAC 地址
SUM	CRC16
0xFF	Tail code

4.28 MCU 查询网络 ID(FC 10)

0xAA 0xAA 0x01 0xFC 0x10 0x00 0x00 SEQ NID SUM 0xFF

字段	含义
0xAA 0xAA	Preamble
0x01	Payload 长度
0xFC	功能码
0x10	查询网络标识子功能码
0x00	Resv1
0x00	Resv2
SEQ	报文序列号 (MCU 维护, 递增)
SUM	CRC16
0xFF	Tail code

4.29 模块回复网络 ID(FD 10)

0xAA 0xAA 0x01 0xFD 0x10 0x00 0x00 SEQ NID SUM 0xFF

字段	含义
0xAA 0xAA	Preamble
0x01	Payload 长度
0xFD	功能码
0x10	回复网络标识子功能码
0x00	Resv1
0x00	Resv2
SEQ	报文序列号 (MCU 维护, 递增)
NID	网络标识
SUM	CRC16
0xFF	Tail code



4.30 MCU 设置工作频段(FE 1C)

0xAA 0xAA 0x02 0xFE 0x1C 0x00 0x00 SEQ BAND_ID SUM 0xFF

字段	含义
0xAA 0xAA	Preamble
0x02	Payload 长度
0xFE	功能码
0x11	MCU 设置工作频段子功能码
0x00	Resv1
0x00	Resv2
SEQ	报文序列号 (MCU 维护, 递增)
BAND_ID	工作频段索引, 设置范围0~4, 8~11
SUM	CRC16
0xFF	Tail code

BAND_ID 与各频段对应关系如下表:

编号	频段
band 0	1.953 - 11.962 MHz
band 1	2.441 - 5.615 MHz
band 2	0.781 - 2.930 MHz
band 3	1.758 - 2.930 MHz
band 4	5.639 - 11.962 MHz
band 8	5.859 - 9.033 MHz
band 9	4.883 - 24.413 MHz
band 10	28.319 - 34.544 MHz
band 11	4.883 - 12.206 MHz

4.31 MCU 设置扫描频段(FE 1E)

0xAA 0xAA 0x03 0xFE 0x1E 0x00 0x00 SEQ BITMAP0 BITMAP1 SUM 0xFF

字段	含义
0xAA 0xAA	Preamble
0x03	Payload 长度
0xFE	功能码
0x1E	MCU 设置扫描频段范围子功能码
0x00	Resv1
0x00	Resv2
SEQ	报文序列号 (MCU 维护, 递增)
BITMAP0~1	16 位扫描工作频段位图
SUM	CRC16
0xFF	Tail code

4.32 MCU 查询扫描频段(FC 14)



0xAA 0xAA 0x02 0xFC 0x14 0x00 0x00 SEQ SCAN_EN SUM 0xFF

字段	含义
0xAA 0xAA	Preamble
0x02	Payload 长度
0xFC	功能码
0x14	MCU 查询扫描频段范围子功能码
0x00	Resv1
0x00	Resv2
SEQ	报文序列号 (MCU 维护, 递增)
SCAN_EN	0—查询模块支持频段, 1—查询扫频范围
SUM	CRC16
0xFF	Tail code



4.33 模块回复扫描频段(FD 14)

0xAA 0xAA 0x03 0xFD 0x14 0x00 0x00 SEQ SCAN_EN BITMAP0~1 SUM 0xFF

字段	含义
0xAA 0xAA	Preamble
0x03	Payload 长度
0xFD	功能码
0x14	MCU 设置扫描频段范围子功能码
0x00	Resv1
0x00	Resv2
SEQ	报文序列号 (MCU 维护, 递增)
SCAN_EN	0—回复模块支持频段, 1—回复扫描范围
BITMAP0~1	频段范围位图, 2 字节, 低位在前
SUM	CRC16
0xFF	Tail code

4.34 MCU 查询模块信息(FC 12)

0xAA 0xAA 0x01 0xFC 0x12 0x00 0x00 SEQ SUM 0xFF

字段	含义
0xAA 0xAA	Preamble
0x01	Payload 长度
0xFC	功能码
0x12	MCU 查询模块信息子功能码
0x00	Resv1
0x00	Resv2
SEQ	报文序列号 (MCU 维护, 递增)
SUM	CRC16
0xFF	Tail code

4.35 模块回复本地基本信息(FD 12)

0xAA 0xAA 0x15 0xFD 0x12 0x00 0x00 SEQ ROLE MAC0~5 STATE NID CCO_MAC0~5 WL_STATE VERO~3 SUM 0xFF

字段	含义
0xAA 0xAA	Preamble
0x15	Payload 长度
0xFD	功能码
0x12	模块回复本地信息子功能码
0x00	Resv1
0x00	Resv2
SEQ	报文序列号 (MCU 维护, 递增)
ROLE	模块网络角色: 1--STA, 2--PCO, 4--CCO



MAC0~5	6 字节模块MAC 地址
STATE	模块启动状态：0—未就绪，1—就绪
NID	网络标识
CCO_MAC0~5	6 字节入网CCO 的地址
WL_STATE	白名单使能或者禁用
VER0~3	4 字节软件版本号
SUM	CRC16
0xFF	Tail code

4.36 查询白名单状态(FC 11)

0xAA 0xAA 0x01 0xFC 0x11 0x00 0x00 SEQ SUM 0xFF

字段	含义
0xAA 0xAA	Preamble
0x01	Payload 长度
0xFC	功能码
0x11	查询白名单状态子功能码
0x00	Resv1
0x00	Resv2
SEQ	报文序列号 (MCU 维护, 递增)
SUM	CRC16
0xFF	Tail code

4.37 回复白名单状态(FD 11)

0xAA 0xAA 0x02 0xFD 0x11 0x00 0x00 SEQ TYPE SUM 0xFF

字段	含义
0xAA 0xAA	Preamble
0x02	Payload 长度
0xFD	功能码
0x11	回复白名单状态子功能码
0x00	Resv1
0x00	Resv2
SEQ	报文序列号 (MCU 维护, 递增)
TYPE	0:关闭1: 打开
SUM	CRC16
0xFF	Tail code

4.38 设置发射功率(FE 16)

0xAA 0xAA 0x02 0xFE 0x16 0x00 0x00 SEQ TXPWR SUM 0xFF

字段	含义
0xAA 0xAA	Preamble
0x02	Payload 长度



0xFE	功能码
0x16	设置发射功率子功能码
0x00	Resv1
0x00	Resv2
SEQ	报文序列号 (MCU 维护, 递增)
TXPWR	设置发射功率值 (有效值范围95 ~ 137)
SUM	CRC16
0xFF	Tail code

4.39 查询发射功率(FC 0B)

0xAA 0xAA 0x01 0xFC 0x0B 0x00 0x00 SEQ SUM 0xFF

字段	含义
0xAA 0xAA	Preamble
0x01	Payload 长度
0xFC	功能码
0x0B	查询发射功率子功能码
0x00	Resv1
0x00	Resv2
SEQ	报文序列号 (MCU 维护, 递增)
SUM	CRC16
0xFF	Tail code

4.40 回复发射功率(FD 0B)

0xAA 0xAA 0x02 0xFD 0x0B 0x00 0x00 SEQ TXPWR SUM 0xFF

字段	含义
0xAA 0xAA	Preamble
0x02	Payload 长度
0xFD	功能码
0x0B	回复发射功率子功能码
0x00	Resv1
0x00	Resv2
SEQ	报文序列号 (MCU 维护, 递增)
TXPWR	返回发射功率值
SUM	CRC16
0xFF	Tail code

4.41 查询 CCO 工作频段(FC 16)

0xAA 0xAA 0x01 0xFC 0x16 0x00 0x00 SEQ SUM 0xFF



字段	含义
0xAA 0xAA	Preamble
0x01	Payload 长度
0xFC	功能码
0x16	查询CCO 工作频段子功能码
0x00	Resv1
0x00	Resv2
SEQ	报文序列号 (MCU 维护, 递增)
SUM	CRC16
0xFF	Tail code

4.42 回复 CCO 工作频段 (FD 16)

0xAA 0xAA 0x02 0xFD 0x16 0x00 0x00 SEQ BAND SUM 0xFF

字段	含义
0xAA 0xAA	Preamble
0x02	Payload 长度
0xFD	功能码
0x16	回复CCO 工作频段子功能码
0x00	Resv1
0x00	Resv2
SEQ	报文序列号 (MCU 维护, 递增)
BAND	返回CCO 工作频段
SUM	CRC16
0xFF	Tail code

4.43 查询节点信息(FC 17)

此命令可以通过mac 地址查询网络中某个节点或所有节点的一些信息, 如果此节点不在网络中, 返回信息为空。

如果 mac 地址为FF FF FF FF FF FF 表示查询当前网络中所有节点的信息。根据查询类型返回相应的一些信息, 详见FD 17 返回节点信息。

0xAA 0xAA 0x07 0xFC 0x17 0x00 TYPE SEQ MACO[~]5 SUM 0xFF

字段	含义
0xAA 0xAA	Preamble
0x07	Payload 长度
0xFC	功能码
0x17	查询节点信息子功能码
0x00	Resv1
TYPE	查询节点信息类型1-5, 详见回复节点信息中的节点返回
SEQ	报文序列号 (MCU 维护, 递增)
MACO [~] 5	查询对应mac 节点对应的信息, mac 地址全F 为查询当前网络所有节点信息。
SUM	CRC16
0xFF	Tail code



4.44 回复节点信息 (FD 17)

查询单个节点返回总条数为1, COUNT 为1, INDEX 为0, NODE_INFO 根据TYPE 决定。查询全网时, 根据实际情况返回总条数, 本次返回几条, 当前返回的序号。

0xAA 0xAA LEN 0xFD 0x17 0x00 TYPE SEQ TOTAL_L TOTAL_H COUNT INDEX NODE_INFO SUM 0xFF

字段	含义
0xAA 0xAA	Preamble
LEN	Payload 长度
0xFD	功能码
0x17	回复节点信息子功能码
0x00	Resv1
TYPE	回复节点信息类型1-5
SEQ	报文序列号 (MCU 维护, 递增)
TOTAL_L	返回节点信息数量, 低字节
TOTAL_H	返回节点信息数量, 高字节
COUNT	当前帧数据中包含节点信息条数
INDEX	返回信息序号, 从0 开始计数
NODE_INFO	节点信息, 详细信息见下表
SUM	CRC16
0xFF	Tail code

节点信息:

类型	返回信息包含						
V1	Mac0 ⁵ 6 字节	节点tei 2 字节	代理节点tei 2 字节				
V2	Mac0 ⁵ 6 字节	上行通信成功率 1 字节	下行通信成功率 1 字节	版本号 4 字节	厂商标识 2 字节	设备类型 1 字节	信噪比 1 字节
V3	Mac0 ⁵ 6 字节	关联请求次数 2 字节	代理变更请求次数 2 字节		接收代理变更次数 4 字节		
V4	Mac0 ⁵ 6 字节	节点在网时间, 4 字节小端, 秒		上一次发现节点所过时间, 4 字节小端, 秒			
V5	Mac0 ⁵ 6 字节	上一次联请求所过时间, 4 字节小端, 秒		上一次代理变更所过时间, 4 字节小端, 秒			



第5章 CRC16 生成方法

```
uint16_t ge_frm_checksum_calc (uint8_t *data, uint16_t len)
{
    register uint16_t crc = 0xFFFF;

    IOT_ASSERT(data && len);

    while (len-- > 0) {
        crc = (crc >> 8) ^ iot_crc16_tab[(crc ^ *data++) & 0xff];
    }

    return crc;
}

/* CRC table for the CRC-16. */
/* The poly is 0x8005 (x^16 + x^15 + x^2 + 1) */ const uint16_t
iot_crc16_tab[256] = {
    0x0000, 0xC0C1, 0xC181, 0x0140, 0xC301, 0x03C0, 0x0280, 0xC241,
    0xC601, 0x06C0, 0x0780, 0xC741, 0x0500, 0xC5C1, 0xC481, 0x0440,
    0xCC01, 0x0CC0, 0x0D80, 0xCD41, 0x0F00, 0xCF41, 0xCE81, 0x0E40,
    0x0A00, 0xCAC1, 0xCB81, 0x0B40, 0xC901, 0x09C0, 0x0880, 0xC841,
    0xD801, 0x18C0, 0x1980, 0xD941, 0x1B00, 0xDB41, 0xDA81, 0x1A40,
    0x1E00, 0xDE41, 0xDF81, 0x1F40, 0xDD01, 0x1DC0, 0x1C80, 0xDC41,
    0x1400, 0xD4C1, 0xD581, 0x1540, 0xD701, 0x17C0, 0x1680, 0xD641,
    0xD201, 0x12C0, 0x1380, 0xD341, 0x1100, 0xD1C1, 0xD081, 0x1040,
    0xF001, 0x30C0, 0x3180, 0xF141, 0x3300, 0xF3C1, 0xF281, 0x3240,
    0x3600, 0xF6C1, 0xF781, 0x3740, 0xF501, 0x35C0, 0x3480, 0xF441,
    0x3C00, 0xFC41, 0xFD81, 0x3D40, 0xFF01, 0x3FC0, 0x3E80, 0xFE41,
    0xFA01, 0x3AC0, 0x3B80, 0xFB41, 0x3900, 0xF9C1, 0xF881, 0x3840,
    0x2800, 0xE8C1, 0xE981, 0x2940, 0xEB01, 0x2BC0, 0x2A80, 0xEA41,
    0xEE01, 0x2EC0, 0x2F80, 0xEF41, 0x2D00, 0xEDC1, 0xEC81, 0x2C40,
    0xE401, 0x24C0, 0x2580, 0xE541, 0x2700, 0xE7C1, 0xE681, 0x2640,
```



0x2200, 0xE2C1, 0xE381, 0x2340, 0xE101, 0x21C0, 0x2080, 0xE041,
0xA001, 0x60C0, 0x6180, 0xA141, 0x6300, 0xA3C1, 0xA281, 0x6240,
0x6600, 0xA6C1, 0xA781, 0x6740, 0xA501, 0x65C0, 0x6480, 0xA441,
0x6C00, 0xACC1, 0xAD81, 0x6D40, 0xAF01, 0x6FC0, 0x6E80, 0xAE41,
0xAA01, 0x6AC0, 0x6B80, 0xAB41, 0x6900, 0xA9C1, 0xA881, 0x6840,
0x7800, 0xB8C1, 0xB981, 0x7940, 0xBB01, 0x7BC0, 0x7A80, 0xBA41,
0xBE01, 0x7EC0, 0x7F80, 0xBF41, 0x7D00, 0xBDC1, 0xBC81, 0x7C40,

0xB401, 0x74C0, 0x7580, 0xB541, 0x7700, 0xB7C1, 0xB681, 0x7640,
0x7200, 0xB2C1, 0xB381, 0x7340, 0xB101, 0x71C0, 0x7080, 0xB041,
0x5000, 0x90C1, 0x9181, 0x5140, 0x9301, 0x53C0, 0x5280, 0x9241,
0x9601, 0x56C0, 0x5780, 0x9741, 0x5500, 0x95C1, 0x9481, 0x5440,
0x9C01, 0x5CC0, 0x5D80, 0x9D41, 0x5F00, 0x9FC1, 0x9E81, 0x5E40,
0x5A00, 0x9AC1, 0x9B81, 0x5B40, 0x9901, 0x59C0, 0x5880, 0x9841,
0x8801, 0x48C0, 0x4980, 0x8941, 0x4B00, 0x8BC1, 0x8A81, 0x4A40,
0x4E00, 0x8EC1, 0x8F81, 0x4F40, 0x8D01, 0x4DC0, 0x4C80, 0x8C41,
0x4400, 0x84C1, 0x8581, 0x4540, 0x8701, 0x47C0, 0x4680, 0x8641,
0x8201, 0x42C0, 0x4380, 0x8341, 0x4100, 0x81C1, 0x8081, 0x4040

};



第6章 附录：常用定义

附录 1 设置命令出错原因

ERR NUM	错误原因:	
0x01	PROTO_REASON_STA_LEAVE_ERR	STA 离线出错
0x02	PROTO_REASON_WL_LOST_FRM	白名单数据帧丢失
0x03	PROTO_REASON_WL_SEQ_MISMATCH	白名单数据帧序号不匹配
0x04	PROTO_REASON_WL_CLR_NOTSUPPORT	不支持白名单清除操作
0x08	PROTO_REASON_NID_DUP	重复的NID
0x09	PROTO_REASON_TIME_OUT	命令超时
0x0A	PROTO_REASON_MAC_MISMATCH	MAC 地址不匹配
0x0B	PROTO_REASON_PWD_MISMATCH	密码不匹配
0x0C	PROTO_REASON_JOINED	已经加入网络
0x0D	PROTO_REASON_NO_AUTHORITY	没有权限
0x0E	PROTO_REASON_LEN_MISMATCH	长度不匹配
0x0F	PROTO_REASON_NID_MISMATCH	NID 不匹配
0x10	PROTO_REASON_CCO_GROUPNETING	CCO 组网中
0x11	PROTO_REASON_CCO_GROUPNETING_IDLE	CCO 不在组网状态
0x12	PROTO_REASON_ERR_DEVTYPE	错误的设备类型
0x13	PROTO_REASON_MAC_ADDR_ZERO	无效的MAC 地址
0x14	PROTO_REASON_NO_MAC_SETTED	MAC 地址未设置
0x15	PROTO_REASON_DUP_SETTING	重复设置
0x16	PROTO_REASON_ROLE_MISMATCH	角色不匹配
0x17	PROTO_REASON_CMD_DIR_ERR	命令的方向不对
0x18	PROTO_REASON_NOT_READY	状态没有准备好
0x19	PROTO_REASON_ALLOC_MEM_ERR	申请内存空间失败
0x1A	PROTO_REASON_NO_NB_NW_FOUND	没有找到邻居网络
0x1B	PROTO_REASON_MONITOR_EXCESS	监控器超过最大支持数量
0x1C	PROTO_REASON_PARAME_ERR	参数错误
0x1D	PROTO_REASON_BAUD_IDX_OOR	波特率编号超出范围
0x1E	PROTO_REASON_SWITCH_UART_MODE_ERR	切换UART 到GE 模式错误
0x1F	PROTO_REASON_SET_HOST_PORT_ERR	设置通信接口错误
0x20	PROTO_REASON_NOT_SUPPORT	不支持
其他	保留	