**APP WiFi热点配网模式通讯协议**

1. **AP/BLE模式配网通讯方式：**

手机app

WiFi采集器（处于AP热点/BLE模式）

TCP

**操作流程：**

**WiFi模式连接：**

1. 手机打开WiFi，采集器处于WiFi热点模式下；
2. 手机连接采集器的WiFi热点；
3. 连接WiFi热点后，手机app发起TCP连接采集器的IP（默认：192.168.10.100）和端口（5280）；
4. 建立TCP连接后，通讯数服协议进行数据通讯（设置、读取等）

**BLE模式连接：**

1. 手机打开BLE，采集器处于BT热点模式下；
2. 手机连接采集器的BLE；
3. 连接BLE热点后，采用直传模式通过数服协议进行数据通讯（设置、读取等）

**配网命令发送流程：**

发送获取周围路由列表命令

设置路由或密码信息并收到应答

连接WiFi热点/BLE

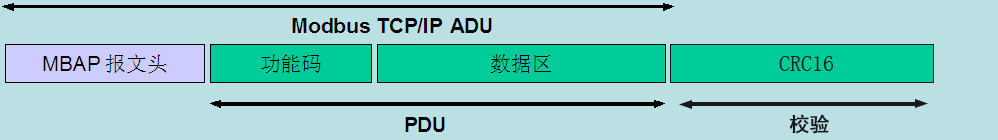
等待采集器返回连接WiFi状态，并收到应答

收到WiFi连接成功应答后，去获取服务器连接状态

发送重启并收到应答

收到WiFi连接失败应答后，提示重新配网，按照流程操作一遍

1. **通讯协议说明**
2. **命令格式**



MBAP报文头：

|  |  |  |
| --- | --- | --- |
| **名称** | **长度** | **描述** |
| 报文编号 | 2字节 | 默认：00 01 |
| 协议标识 | 2字节 | 00 05 |
| 数据长度 | 2字节 | 更具数据内容定 |
| 从站地址 | 1字节 | 默认：01 |

功能码：

|  |  |  |
| --- | --- | --- |
| **Code** | **长度** | **描述** |
| 0x17 | 1字节 | 透传命令码，用来与逆变器数据通讯（03/04/06/10） |
| 0x18 | 1字节 | 设置采集器参数 |
| 0x19 | 1字节 | 获取采集器参数 |

数据区：

各个功能码下有不同的数据区，因此数据区的长度和内容不是固定不变的。本协议对数据区的描述是按功能码分别进行描述的，详见“协议内容”章节对各个功能码部分的描述；

注意：数去发送前需要对数据区进行一个数据加密运算，算法如下

数据区异或加密：

（1）秘钥： “Growatt”

（2）加密方式：

加密采用数据区循环异或秘钥的方式，加密后进行CRC运算。

命令包做AES-CBC加密：

（1）秘钥： “\_growatt\_datalog”

（2）加密方式：

加密采用整命令包进行AES-CBC加密，数据个数需要整除16，不足数据包后面补0x00。

校验区（CRC16）：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 通讯校验 | 2字节  （CRC16值高字节在前，低字节在后） | CRC16校验，在前面的数据后，增加两字节CRC16检验，CRC校验不计入长度，校验方法见附件 | 由客户端生成 | 服务端在应答时重新生成 | 5.0之后的版本,在数据区加密后再进行校验； |

1. **通讯协议命令码（0x17、0x18、0x19、0x26）**
2. **命令码0x17**

该功能码为完全透传命令：由手机app发送该命令码，数据采集器收到该命令码后，取出“透传数据区”，不作协议转换地透传给光伏设备；同时，对光伏设备返回的数据同样不作任何解析，直接当作“透传数据区”封装在MODBUS\_ TCP协议中响应给网络服务器。

该命令并不局限于数据查询，还可以进行数据设置；也并不局限于对逆变器适用，对其它通过数据采集器与手机app相连的光伏设备同样适用，只要光伏设备能够解析出“透传数据区”中的内容，同时手机app也能解析出响应命令中“透传数据区”中的内容即可。

手机app发往数据采集器的命令格式如下表所示：

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **报文头** | | | | | **功能码** | **数据区** | | |
| 通讯编号 | | 协议标识 | 数据长度 | 设备地址 |  | 数据采集器序列号 | 透传数据区的数据长度 | 透传数据区 |
| 0x00 | 0x01 | 00 05 | 2字节，根据实际情况计算 | 01 | 0x17 | 10字节 | 2字节 | 数据长度由“透传数据区的数据长度”指定，数据内容参见逆变器modbus协议 |

数据采集器在收到手机app的该功能码后，需判断命令的合法性，然后执行对应的设置操作，最后给网络服务器返回响应：

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **报文头** | | | | | **功能码** | **数据区** | | |
| 通讯编号 | | 协议标识 | 数据长度 | 设备地址 |  | 数据采集器序列号 | 透传数据区的  数据长度 | 透传数据区 |
| 0x00 | 0x01 | 00 05 | 2字节，根据实际情况计算 | 01 | 0x17 | 10字节 | 2字节 | 数据长度由“透传数据区的数据长度”指定，数据内容参见逆变器modbus协议 |

1. **命令码0x18**

该功能码是手机app与数据采集器之间的命令，它用于手机app对数据采集器的相关参数进行设置，一次可对单/多个参数进行设置。

手机app发往数据采集器的命令格式如下表所示：

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **报文头** | | | | | **功能码** | **数据区** | | | |
| 通讯编号 | | 协议标识 | 数据长度 | 设备地址 |  | 数据采集器序列号 | 参数编号个数 | 设置数据的长度 | 设置数据 |
| 0x00 | 0x01 | 00 05 | 2字节，根据实际情况计算 | 0x01 | 0x18 | 10字节 | 2字节 | 2字节 | 参数格式如下 |

参数格式列表：

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 参数编号1 | 参数长度 | 参数数据 | 参数编号2 | | | 参数编号3 | | | 参数编号n | | |
| 2字节 | 2字节 | 由参数长度决定 |  |  |  |  |  |  |  |  |  |

数据采集器在收到手机app的该功能码后，需判断命令的合法性，然后执行对应的设置操作，最后给网络服务器返回响应：

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **报文头** | | | | | | **功能码** | **数据区** | | |
| 通讯编号 | | 协议标识 | 数据长度 | | 设备地址 |  | 数据采集器序列号 | 参数编号个数 | 状态码 |
| 0x00 | 0x01 | 00 05 | 0x00 | 0x0F | 0x01 | 0x18 | 10字节 | 2字节 | 1字节，参见下表 |

状态码列表：

|  |  |  |
| --- | --- | --- |
| **状态码** | **释义** | **备注** |
| 0x00 | 成功 | 数据采集器接收到该命令后，经判断，设置数据合法，且对应的所有寄存器均可写，视为成功。此时，手机app需提示用户设置成功。 |
| 0x01 | 设置数据不合法 | 数据采集器接收到该命令后，经判断，设置数据不合法，如数据长度不正确，数据超过有效数据范围，终止寄存器小于起始寄存器等等，视为设置数据不合法。此时，手机app需提示用户设置错误。 |

**2、命令码0x19**

该功能码是手机app与数据采集器之间的命令，它用于手机app对数据采集器的相关参数进行读取，一次可对单/多个参数进行读取。

手机app发往数据采集器的命令格式如下表所示：

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **报文头** | | | | | **功能码** | **数据区** | | |
| 通讯编号 | | 协议标识 | 数据长度 | 设备地址 |  | 数据采集器序列号 | 参数编号个数 | 设置数据 |
| 0x00 | 0x01 | 00 05 | 2字节，根据实际情况计算 | 0x01 | 0x19 | 10字节 | 2字节 | 参数格式如下 |

参数格式列表：

|  |  |  |  |
| --- | --- | --- | --- |
| 参数编号1 | 参数编号2 | 参数编号3 | 参数编号n |
| 2字节 |  |  |  |

数据采集器在收到手机app的该功能码后，需判断命令的合法性，然后执行对应的设置操作，最后给网络服务器返回响应。

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **报文头** | | | | | **功能码** | **数据区** | | | |
| 通讯编号 | | 协议标识 | 数据长度 | 设备地址 |  | 数据采集器序列号 | 参数编号个数 | 状态码 | 获取到  有效数据 |
| 0x00 | 0x01 | 00 05 | 2字节，根据实际情况计算 | 0x01 | 0x19 | 10字节 | 2字节 | 1字节，参见下表 | 格式参考下表 |

状态码列表：

|  |  |  |
| --- | --- | --- |
| **状态码** | **释义** | **备注** |
| 0x00 | 成功 | 数据采集器接收到该命令后，经判断，设置数据合法，且对应的所有寄存器均可写，视为成功。此时，手机app需提示用户设置成功。 |
| 0x01 | 设置数据不合法 | 数据采集器接收到该命令后，经判断，设置数据不合法，如数据长度不正确，数据超过有效数据范围，终止寄存器小于起始寄存器等等，视为设置数据不合法。此时，手机app需提示用户设置错误。 |

参数格式列表：

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 参数编号1 | 参数长度 | 参数数据 | 参数编号2 | | | 参数编号3 | | | 参数编号n | | |
| 2字节 | 2字节 | 由参数长度决定 |  |  |  |  |  |  |  |  |  |

1. **功能码38（0x26）**

该功能码是网络服务器给采集器下发文件用于采集器或逆变器升级。目前仅WIFI-S/WIFI-X类型采集器采用此方式。流程逻辑：~~1、设置采集器为升级模式；~~2、查询采集器需要的升级文件类型；3、发送升级文件包：服务器以0x26开始文件传输-->完成后；按原有升级流程采集器.

### 网络服务器发送的数据格式

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **报文头** | | | | | **功能码** | **数据区** | | |
| 通讯编号 | | 协议标识 | 数据长度 | 设备地址 |  | 数据采集器序列号 | 数据串  长度 | **数据区段** |
| 0x00 | 0x01 | 00 05 | 2字节，根据实际情况计算 | 01 | 0x26 | 10字节 | 2字节，根据“逗号数据串”的长度填写 | 见下表 |

网络服务器发往数据采集器的命令格式如下表所示：

网络服务器对数据采集器的文件发送命令格式

|  |  |  |
| --- | --- | --- |
| **数据区段定义字节** | **逗号字段描述** | **备注** |
| 00 - 01 | 文件数据分包总数量 |  |
| 02 - 03 | 当前数据包编号 | 从1开始 |
| 04 - xx | 文件数据包数据 | 每包数据包长度根据实际定义，WiFi通讯：2048byte，BLE通讯：256byte |

### 采集器回复的数据格式

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **报文头** | | | | | | **功能码** | **数据区** | |
| 通讯编号 | | 协议标识 | 数据长度 | | 设备地址 |  | 数据采集器序列号 | 数据 |
| 0x00 | 0x01 | 00 05 | 0x00 | 0x11 | 01 | 0x26 | 10字节 | 5字节，见下表 |

网络服务器对数据采集器的回复命令格式

|  |  |  |
| --- | --- | --- |
| **数据区段定义字节** | **逗号字段描述** | **备注** |
| 00 - 01 | 文件数据分包总数量 |  |
| 02 - 03 | 当前数据包编号 | 从1开始 |
| 04 | 当前数据包接收状态码 |  |

|  |  |  |
| --- | --- | --- |
| 接收状态**码** | **释义** | **备注** |
| 0 | 成功 | 服务器发送下一包 |
| 1 | 接收异常 | 服务器再次发送当前包 |
| 2 | 整体检验错误 | 重新发送文件第一包 |
| 3 | 其他错误（采集器准备失败） | 重新发送文件第一包 |

**采集器参数说明：**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **参数编号** | **参数名称** | **适用数据采集器类型** | **解说** | **读写属性** | **备注**  **（以下描述均为字符串表述）** |
| 04 | Data Interval | ShineWiFi-S/-X | 数据采集器向网络服务器传送数据的间隔时间，单位为分钟 | R/W | 取值范围：[0.1, 60.0]，默认为5。  如字符5表示间隔时间为5分钟。小数位最多支持1位。 |
| 08 | Datalogger SN | ShineWiFi-S/-X | 数据采集器序列号 | R/W | 数据采集器序列号，例：  序列号是0123456789，则传输时  Datalogger SN = 0x30 0x31 0x32  0x33 0x34 0x35 0x36 0x37 0x38 0x39 |
| 13 | Datalogger Type | ShineWiFi-S/-X | 数据采集器类型 | R/W | 固定1个字符，编码定义如下：  11：ShineWiFi-S  16：ShineWiFi-X |
| 14 | Local IP | ShineWiFi-S/-X | 数据采集器的本端IP地址 | R/W | 最大15个字符，默认：192.168.5.1 |
| 16 | Local Mac | ShineWiFi-S/-X | 数据采集器连入互联网的网卡MAC地址 | R | 17个字符， 格式如： 12:34:56:78:90:AB |
| 17 | Remote IP | ShineWiFi-S/-X | 数据采集器的远端（网络服务器）IP地址 | R/W |  |
| 18 | Remote Port | ShineWiFi-S/-X | 数据采集器的远端（网络服务器）端口 | R/W | 默认值：5279  默认值：server.growatt.com |
| 19 | Remote URL | ShineWiFi-S/-X | 数据采集器的远端（网络服务器）域名 | R/W |
| 21 | Firmware Version | ShineWiFi-S/-X | 数据采集器的固件版本 | R | 采用四段表示法，如：1.2.3.4 |
| 22 | Hardware Version | ShineWiFi-S/-X | 数据采集器的硬件版本 | R |  |
| 25 | SubnetMask | ShineWiFi-S/-X | 数据采集器的子网掩码 | R/W | 最大15个字符，默认：255.255.255.0 |
| 26 | DefaultGateway | ShineWiFi-S/-X | 数据采集器的默认网关 | R/W | 最大15个字符，默认：192.168.5.1 |
| 31 | System Time | ShineWiFi-S/-X | 数据采集器的系统时间 | R/W | 固定19个字符，格式为：yyyy-MM-dd HH:mm:ss |
| 32 | Datalogger Restart | ShineWiFi-S/-X | 数据采集器重启标识 | R/W | 固定1个字符，编码定义如下：  0：正常工作  1：重启数据采集器  默认为0，当设置为1时，重启数据采集器，重启后，该寄存器恢复到默认值 |
| 56 | WiFi SSID | ShineWiFi-S/-X | WIFI 模块要链接热点名称 | R/W | 存储WiFi模块要链接的无线SSID |
| 57 | WiFi Password | ShineWiFi-S/-X | WIFI 模块要链接的热点密钥 | R/W | 存储WiFi模块要链接的无线密钥 |
| 60 | Link status | ShineWiFi-S/-X | WiFi连接状态 | R | 0-255 0:连接成功  1-255:: 连接失败 201：路由名字错误 204：路由密码错误 |
| 65 | Fota File Type | ShineWiFi-S/-X | WiFi升级文件类型 | R | 返回值1/2，int类型 1：user1.bin  2：user2.bin |
| 71 | Net DHCP | ShineWiFi-S/-X | DHCP使能 | R/W | = ‘1’,使能DHCP  = ‘0’,不使能DHCP |
| 75 | get router name | ShineWiFi-S/-X | 获取周围路由WiFi名字 | R/W | 内容：名字（字符） + 信号rssi（值）  整体数据格式：  总路由器个数（1 byte）+第1个路由字符长度（1 byte）+第1个路由字符（不定 byte）+第1个路由信号值（1 byte） … +第n个路由字符长度（1 byte）+第n个路由字符（不定 byte）+第n个路由信号值（1 byte） |

**变更记录：**

**Isen 2020.12.23 V1.0**

1. 增加60号寄存器，用来上报WiFi连接状态；
2. 配网命令发送流程简单说明；

**Isen 2021.01.15 V1.1**

1. 增加0x26命令码，用来下发升级文件数据；
2. 增加65号寄存器，用来上报WiFi本地升级下发文件类型值；

**Isen 2021.11.29 V1.2**

1、兼容蓝牙通讯方式兼容，增加AES-CBC对命令数据包加密；