

机智云平台标准接入协议

之App与设备通讯

(v4.0.7)

修订历史

版本	修订内容	修订人	修订日期
4.0.0	V4版协议	刘冠华	2014-11-17
4.0.1	更正文档错误：移除透传业务指令中的“业务指令长度”字段	刘冠华	2014-12-15
4.0.2	添加App请求WiFi模组退出产测模式指令	刘冠华	2014-12-26
4.0.3	添加配置成功广播（AirLink方式）	刘冠华	2015-01-05
4.0.4	“设备发现响应”及“设备上电广播”包中增加“设备属性”字段，用于标识设备是否为中控设备	刘冠华	2015-02-15
4.0.5	添加“透传业务指令（带ACK）”	刘冠华	2015-04-18
4.0.6	更正文档中的错别字	刘冠华	2015-06-04
4.0.7	更新“透传业务指令（带ACK）”的“业务指令”字段说明：如本ACK消息不携带任何消息内容，本字段为空； 明确当“透传业务指令（带ACK）”的包序号不为0时才需要ACK； 取消“App读取设备信息”的固件Fid字段和固件版本号字段的意义，定为保留字段；	刘冠华	2015-06-15

目录

[通讯模型](#)

[通讯流程](#)

[安全策略](#)

[约定](#)

[通讯协议](#)

[配置设备\(SoftAP方式\)](#)

[配置成功广播\(AirLink方式\)](#)

[发现设备](#)

[绑定设备](#)

[登陆设备](#)

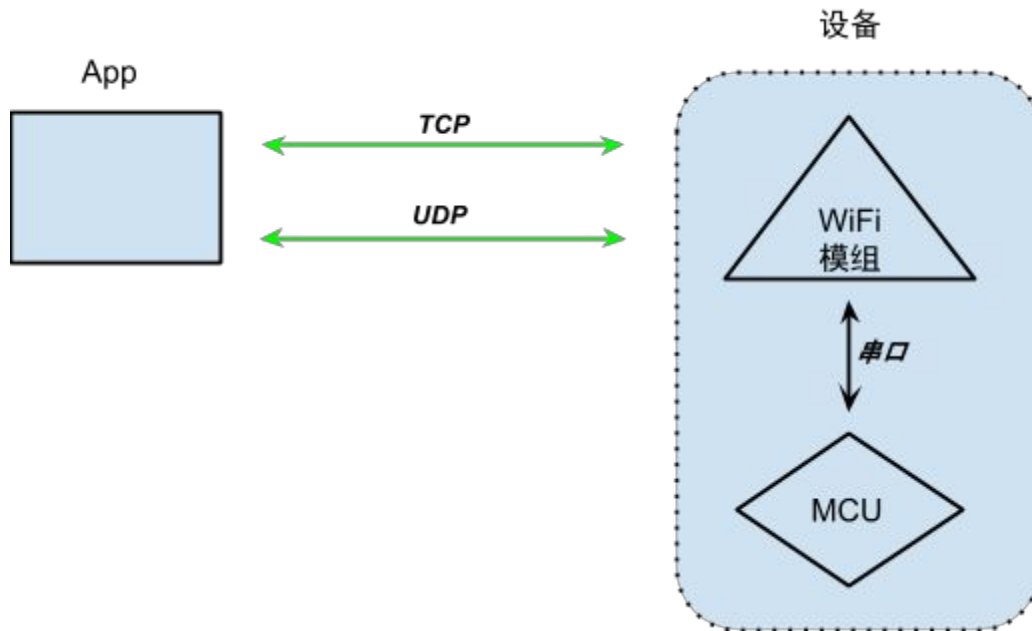
[透传业务指令](#)

[透传业务指令（带ACK）](#)

[App请求设备查询WiFi热点列表](#)
[App设置设备的日志级别与指示灯开关](#)
[设备向App发送日志](#)
[App读取设备信息](#)
[心跳](#)
[App请求WiFi模组退出产测模式](#)

1. 通讯模型

小循环是指App和设备处于同一个局域网内，通过TCP或UDP方式直接通讯。



WiFi模组的主要作用是以无线的方式透传App与MCU之间的业务指令命令。MCU主要负责处理业务指令。

2. 通讯流程

App与设备的小循环通讯主要包括以下的通信用过程。

- **配置设备。**为设备设置所在局域网的WiFi SSID和密码，让设备通过WiFi接入局域网。设备首次上电时需要这一过程。
- **发现设备。**App发送UDP广播包，设备响应UDP广播包。同时设备上电后也会发送UDP广播宣告自己的存在。App需要发现了设备后才能与设备作进一步的交互。
- **连接设备。**App发现设备后，与设备建立TCP连接。
- **绑定设备。**建立用户与设备的绑定关系，并获得登陆设备的Passcode。用户首次操控设备前需要这一过程。
- **登陆设备。**App与设备建立TCP连接后，需通过在绑定设备时获得的Passcode登陆设备后方可操控设备。

- **操控设备。**App登陆设备后，可以通过与设备之间的TCP连接控制设备和接收设备的状态。

3. 安全策略

为了更好的保护设备免受非法的操控，制定本小循环操作安全策略。

- **绑定设备。**用户能够绑定设备的前提是用户能够物理接触到设备。设备上应设置按钮或组合键让用户触发设备处于可绑定状态。这个可绑定状态会持续一定的时间后超时。设备处于可绑定状态后，用户通过App发现设备，连接设备，并主动向设备查询得到设备的Passcode。
- **登陆设备。**通过App控制设备或接收设备的状态报告前必须先通过Passcode登陆设备。但请注意有些命令是无需登陆设备的，见下文。
- **TCP连接资源的释放。**App连接设备后，不登陆而直接发送控制指令，设备会主动断开该TCP连接。App连接设备后，超过60秒没有向设备发送数据，设备也会主动断开该TCP连接。

4. 约定

4.1. 协议阅读说明

- **可变长度：**由 1 ~ 4 个字节(B)表示本可变长度字段后一直到数据包结尾的字节数。编码解码方式请参考《[MQTT_V3.1_Protocol_Specific.pdf](#)》第6页Remaining Length。
- **长度：**没有注明为可变长度的都为普通长度，一般由一个(1B)或两个字节(2B)组成。若多于一个字节组成，采用大端编码方式，即高字节在前，低字节在后。

4.2. App与设备服务端口号的定义

- 设备监听UDP广播端口号为：**12414**
- 设备TCP服务端口号为：**12416**
- App监听UDP广播端口号为：**2415**

5. 通讯协议

5.1. 配置设备(SoftAP方式)

新设备必须配置连接网络后才能和App和云端通讯，也就是把WiFi SSID和密码发送给设备，让设备接入局域网。

App以UDP广播的方式把局域网的WiFi SSID和密码发送给设备，App ⇒ 设备，UDP广播。

序号	字段名称	字节长度(B)	内容说明
1	固定包头	4	0x00000003
2	可变长度	1~4	len(Flag...密码)

3	Flag	1	0x00
4	命令字	2	0x0001
5	SSID长度	2	len(SSID)
6	SSID	max 32	SSID
7	密码长度	2	len(密码)
8	密码	max 32	密码

设备确认，设备 ⇒ App，UDP单播。设备处于UDP广播的监听状态。当收到App发送的数据后，保存局域网的WiFi SSID和密码后以单播的方式向App返回确认。确认帧发往App所在的IP，端口号为App发广播时所使用的UDP端口号。

序号	字段名称	字节长度(B)	内容说明
1	固定包头	4	0x00000003
2	可变长度	1~4	len(Flag...命令字) = 0x03
3	Flag	1	0x00
4	命令字	2	0x0002

5.2. 配置成功广播(AirLink方式)

设备通过AirLink的方式成功连接上路由器后，需要以广播的方式告知手机已配置成功。

设备广播配置成功消息，设备 ⇒ App，UDP广播。

序号	字段名称	字节长度(B)	内容说明
1	固定包头	4	0x00000003
2	可变长度	1~4	len(Flag...产品标识)
3	Flag	1	0x00
4	命令字	2	0x0019
7	MAC长度	2	len(MAC)
8	MAC	max 32	设备MAC地址
11	产品标识长度	2	len(产品标识)

12	产品标识	max 32	设备的产品标识，同类型设备产品标识号相同。App会根据此字段判断是否支持该设备
5	DID长度	2	len(DID)，如还没有DID，长度填0
6	DID	max 23	设备ID(Device ID)

5.3. 发现设备

App操控设备前，必须要先发现设备并判断是否支持该设备，然后再连接设备和登陆设备。

App在局域网内向设备发送UDP广播，App ⇒ 设备，UDP广播。

序号	字段名称	字节长度(B)	内容说明
1	固定包头	4	0x00000003
2	可变长度	1~4	len(Flag...命令字) = 0x03
3	Flag	1	0x00
4	命令字	2	0x0003

设备回复，设备 ⇒ App，UDP单播。设备处于UDP广播的监听状态。当收到App的发现请求后，以单播的方式回复App。回复发往App所在的IP，端口为App发广播时所使用的UDP端口号。

序号	字段名称	字节长度(B)	内容说明
1	固定包头	4	0x00000003
2	可变长度	1~4	len(Flag...产品标识)
3	Flag	1	0x00
4	命令字	2	0x0004
5	DID长度	2	len(DID)
6	DID	max 23	设备ID(Device ID)
7	MAC长度	2	len(MAC)
8	MAC	max 32	设备MAC地址
9	固件版本号长度	2	len(固件版本号)
10	固件版本号	max 32	设备的固件版本号，本字段用于调试

11	产品标识长度	2	len(产品标识)
12	产品标识	max 32	设备的产品标识，同类型设备产品标识号相同。App会根据此字段判断是否支持该设备
13	设备属性	8	设备属性。从右向左编号成bit0~bit63。bit0=1表示设备是中控设备。bit1~bit63预留

设备上电后会主动向App广播自己的存在，设备 ⇒ App，UDP广播。

序号	字段名称	字节长度 (B)	内容说明
1	固定包头	4	0x00000003
2	可变长度	1~4	len(Flag...产品标识)
3	Flag	1	0x00
4	命令字	2	0x0005
5	DID长度	2	len(DID)
6	DID	max 23	设备ID(Device ID)
7	MAC长度	2	len(MAC)
8	MAC	max 32	设备MAC地址
9	固件版本号长度	2	len(固件版本号)
10	固件版本号	max 32	设备的固件版本号，本字段用于调试
11	产品标识长度	2	len(产品标识)
12	产品标识	max 32	设备的产品标识，同类型设备产品标识号相同。App会根据此字段判断是否支持该设备
13	设备属性	8	设备属性。从右向左编号成bit0~bit63。bit0=1表示设备是中控设备。bit1~bit63预留

5.4. 绑定设备

用户操作设备前，必须要先通过绑定获得设备的操作权限，也就是得到设备的Passcode，通过App向设备询问Passcode的方式进行完成。如设备当前处于可绑定状态，则回复App设备的Passcode，不然则返回错误。设备可通过按键或组合键进入可绑定状态，可绑定状态超过一定时间后会超时。本命令无需App登陆设备即可执行。

App向设备发送请求绑定命令，App ⇒ 设备，TCP。

序号	字段名称	字节长度(B)	内容说明
1	固定包头	4	0x00000003
2	可变长度	1~4	len(Flag...命令字) = 0x03
3	Flag	1	0x00
4	命令字	2	0x0006

设备回复绑定请求，设备 \Rightarrow App，TCP。设备收到App的请求Passcode指令后，判断当前是否处于可绑定状态，如可绑定，则回复Passcode，如不可绑定，回复空的Passcode。

序号	字段名称	字节长度(B)	内容说明
1	固定包头	4	0x00000003
2	可变长度	1~4	len(Flag...Passcode)
3	Flag	1	0x00
4	命令字	2	0x0007
5	Passcode长度	2	可绑定时，值为len(Passcode)；不可绑定时，值为0
6	Passcode	max 32	设备Passcode，仅当设备处于可绑定状态时才有值

5.5. 登陆设备

App向设备发送控制命令前或接收设备状态前必须先登陆设备。登陆设备发生在发现设备并与设备建立TCP连接之后。

App向设备发送登陆请求，App \Rightarrow 设备，TCP。

序号	字段名称	字节长度(B)	内容说明
1	固定包头	4	0x00000003
2	可变长度	1~4	len(Flag...Passcode)
3	Flag	1	0x00
4	命令字	2	0x0008
5	Passcode长度	2	len(Passcode)
6	Passcode	max 32	设备Passcode

设备回复登陆请求，设备 \Rightarrow App，TCP。设备收到App的登陆请求后，对比请求参数中的Passcode是否和当前的Passcode相匹配，并返回登陆结果。如Passcode非法，设备则主动断开与App的TCP连接。

序号	字段名称	字节长度(B)	内容说明
1	固定包头	4	0x00000003
2	可变长度	1~4	len(Flag...结果)
3	Flag	1	0x00
4	命令字	2	0x0009
5	结果	1	登陆结果，0为成功，1为失败

5.6. 透传业务指令

App登陆设备后，App与设备相互间可以发送和接收业务指令。业务指令视具体的产品定制，如开关设备，调节温度，设备上报状态等。

App向设备传送业务指令，App \Rightarrow 设备，TCP。

序号	字段名称	字节长度(B)	内容说明
1	固定包头	4	0x00000003
2	可变长度	1~4	len(Flag...业务指令)
3	Flag	1	0x00
4	命令字	2	0x0090
5	业务指令	max 65535	业务指令

设备向App传送业务指令，设备 \Rightarrow App，TCP。

序号	字段名称	字节长度(B)	内容说明
1	固定包头	4	0x00000003
2	可变长度	1~4	len(Flag...业务指令)
3	Flag	1	0x00
4	命令字	2	0x0091
5	业务指令	max 65535	业务指令

5.7. 透传业务指令（带ACK）

App登陆设备后，App与设备相互间可以发送和接收业务指令。业务指令视具体的产品定制，如开关设备，调节温度，设备上报状态等。

传送业务指令，App ⇒ 设备 或 设备 ⇒ App，TCP。

序号	字段名称	字节长度(B)	内容说明
1	固定包头	4	0x00000003
2	可变长度	1~4	len(Flag...业务指令)
3	Flag	1	0x00
4	命令字	2	0x0093
5	包序号(sn)	4	消息的序号，用于消息的ACK。如值为0x00000000，表示不需要ACK
6	业务指令	max 65535	业务指令

业务指令ACK，设备 ⇒ App 或 App ⇒ 设备，TCP。仅当请求消息的包序号(sn)不为0x00000000才需要本ACK消息。

序号	字段名称	字节长度(B)	内容说明
1	固定包头	4	0x00000003
2	可变长度	1~4	len(Flag...业务指令)
3	Flag	1	0x00
4	命令字	2	0x0094
5	包序号(sn)	4	对应发送包的包序号
6	业务指令	max 65535	业务指令，如本ACK消息不携带任何消息内容，本字段为空

5.8. App请求设备查询WiFi热点列表

通过SoftAP配置设备时，App可以请求设备扫描周围的WiFi热点列表，以方便用户选择。

App请求设备扫描并返回WiFi热点列表。App ⇒ 设备，TCP。

序号	字段名称	字节长度(B)	内容说明
----	------	---------	------

1	固定包头	4	0x00000003
2	可变长度	1~4	len(Flag...命令字)
3	Flag	1	0x00
4	命令字	2	0x000C

设备向App返回WiFi热点列表，设备 ⇒ App，TCP。

序号	字段名称	字节长度(B)	内容说明
1	固定包头	4	0x00000003
2	可变长度	1~4	len(Flag...业务指令)
3	Flag	1	0x00
4	命令字	2	0x000D
5	WiFi热点列表	max 65535	由一个或多个WiFi热点项，每个WiFi热点项请见下面的数据结构

WiFi热点项：

序号	字段名称	字节长度(B)	内容说明
1	SSID长度	2	len(SSID)
2	SSID	max 32	SSID
3	信号强度	1	由数字0~255表示SSID的信息强度，数字越大信号越强

5.9. App设置设备的日志级别与指示灯开关

可以通过App设置设备的日志级别与指示灯开关。

App请求设置设备的日志级别与指示灯开关，App ⇒ 设备，TCP。

序号	字段名称	字节长度(B)	内容说明
1	固定包头	4	0x00000003
2	可变长度	1~4	len(Flag...设置值bit0~bit7)
3	Flag	1	0x00

4	命令字	2	0x0010
5	设置值bit8~bit15	1	bit8 ~ bit15从低位(bit)向高位排列
6	设置值bit0~bit7	1	bit0 ~ bit7从低位(bit)向高位排列，与上面的bit8 ~ bit15一共组成bit0 ~ bit15，各位的定义如下： <ul style="list-style-type: none"> • bit0: Error日志级别的开与关，0为关，1为开 • bit1: Warning日志级别的开与关，0为关，1为开 • bit2: Info日志级别的开与关，0为关，1为开 • bit3: WiFi模组所有指示灯的总开关，0为关，1为开 • bit4~bit15: 保留

设备返回操作结果，设备 ⇒ App，TCP。

序号	字段名称	字节长度(B)	内容说明
1	固定包头	4	0x00000003
2	可变长度	1~4	len(Flag...命令字)
3	Flag	1	0x00
4	命令字	2	0x0011

5.10. 设备向App发送日志

当设备相关的日志级别打开后，设备会主动向连接了的App发送日志。本命令无需App登陆设备即可执行。

设备向App发送日志，设备 ⇒ App，TCP。

序号	字段名称	字节长度(B)	内容说明
1	固定包头	4	0x00000003
2	可变长度	1~4	len(Flag...产品标识码)
3	Flag	1	0x00
4	命令字	2	0x0012
5	日志级别	1	1为Error，2为Warning，3为Info，
6	标签长度	2	len(标签)
7	标签	max 256	指示日志种类与关键字

8	来源长度	2	len(来源)
9	来源	max 32	指示日志是从哪里来的
10	日志内容长度	2	len(日志内容)
11	日志内容	max 65535	日志的内容，为UTF8编码的字符

5.11. App读取设备信息

App在发现设备后可以通过本命令获取设备的版本号等信息。本命令无需App登陆设备即可执行。

App请求设备信息，App ⇒ 设备，TCP。

序号	字段名称	字节长度 (B)	内容说明
1	固定包头	4	0x00000003
2	可变长度	1~4	len(Flag...命令字) = 0x03
3	Flag	1	0x00
4	命令字	2	0x0013

设备向App返回信息。设备 ⇒ App，TCP。

序号	字段名称	字节长度 (B)	内容说明
1	固定包头	4	0x00000003
2	可变长度	1~4	len(Flag...产品标识码)
3	Flag	1	0x00
4	命令字	2	0x0014
5	WiFi模组硬件版本号	8	字符串
6	WiFi模组软件版本号	8	字符串
7	MCU硬件版本号	8	字符串
8	MCU软件版本号	8	字符串
9	业务协议版本号	8	字符串

10	保留区1	8	预留
11	保留区2长度	2	len(保留区2)
12	保留区2	max 32	预留
13	产品标识码长度	2	len(产品标识码)
14	产品标识码	max 32	产品标识码，也称为product_key

5.12. 心跳

当App超过一定时间没有向设备发送数据，需要向设备发送心跳包。App心跳超时时间建议设定为50秒。当App在10秒内没有收到设备的心跳响应，可以认为已断开了与设备的连接。当设备在60秒内没有收到App的心跳请求可以认为与App的连接已断开。请注意本命令需App登陆设备后方可执行。

App向设备发送心跳，App ⇒ 设备，TCP。

序号	字段名称	字节长度(B)	内容说明
1	固定包头	4	0x00000003
2	可变长度	1~4	len(Flag...命令字) = 0x03
3	Flag	1	0x00
4	命令字	2	0x0015

设备向App回复心跳，设备 ⇒ App，TCP。

序号	字段名称	字节长度(B)	内容说明
1	固定包头	4	0x00000003
2	可变长度	1~4	len(Flag...命令字)
3	Flag	1	0x00
4	命令字	2	0x0016

5.13. App请求WiFi模组退出产测模式

App在完成产测后，请求WiFi模组退出产测模式。本命令无需App登陆设备即可执行。

App请求WiFi模组退出产测模式，App ⇒ 设备，TCP。

序号	字段名称	字节长度 (B)	内容说明
1	固定包头	4	0x00000003
2	可变长度	1~4	len(Flag...命令字) =0x03
3	Flag	1	0x00
4	命令字	2	0x0017

设备响应App的请求。设备 ⇒ App, TCP。

序号	字段名称	字节长度 (B)	内容说明
1	固定包头	4	0x00000003
2	可变长度	1~4	len(Flag...命令字) =0x03
3	Flag	1	0x00
4	命令字	2	0x0018