通

信

协

议

V 1.0

目录

约定

1.数据从左至右排列,包头为第一字节，依次类推；
2.每一条完整的命令为一个数据包；
3.16 进制数据模式；
4.通信最大数据长度为 1400 字节。
5.校验算法 CRC16
6.转议码：
发送:
0x55 -> 0x54 0x01
0x54 -> 0x54 0x02
数据报文中，除包头包尾外，其它任何字节出现 0x55 都需要进行转义
接收:
接收:
0x54 0x01 -> 0x55
0x54 0x02 -> 0x54
7.BCD(8421 码)
8. string 以 ‘\0’结束，如:”abc123\0”，字节长度:7Byte
9.设备 ID, 16 进制 MAC 地址(8Byte)
10.指令除有特定回复外，都需要有一个对应的通用回复

协议基本格式

终端收发：
格式（TCP/UDP 通信）

整个包长度，转义之前

Header
Length

CommondCategor
y
CommondWord
CommondIndex
ExtendedInfo
Status
DeviceID
TokenLength
Token

Heade
r

登陆时记录当前时间,之后每次发包都+
+

Footer

长度(Byte)	名称	描述
1	包头	
1	长度低位	
1	长度高位	
1	命令类别	
1	命令字	
1	命令序号低位	
1	命令序号高位	
2	**扩展信息**	包括序号，加密等其它扩展
[9] 1	状态	
[10..17] 8	设备 ID	16 进制 MAC 地址(8Byte),设备号,不足前面补 0
[18] N	Torken	通信令牌，登录成功后才有此字段,第一字节表示长度
[27] N	数据区	传输的数据
1	CRC 低位	
1	CRC 高位	
1	包尾	0X5 5

扩展信息段:

0	**1**
预留扩展,2Byte	

字段说明:

A.包头包尾：0x55；

B.命令长度：整条命令数据的长度，包括“长度”本身及包头包尾,CRC 校验位；

C.CRC：由“包头”至“数据”的所有字节的 CRC16 运算值；

即: 包头,长度:低位,长度:高位,命令类别,命令字,用户 ID，数据。

D. 命令执行状态, 0x00 成功 0x01 失败 0x02 主动发送 0x03 不支持

E. Torken: 除设备发起登录时，不需要发送此字段外，所有其它指令，均需有此字段，设备与服务器在建立连接后，以此字段来区分是否合法链接发来的指令，防止强行伪造信息包。

文档记录

日期	修改人员	描述
2015-07-10	唐登安	增加设备上传紧急数据
2015-07-03	唐登安	增加控制设备与 app 间的局域网内网通信指令
2015-06-16	唐登安	增加设备请求移除自身与用户的关联
2015-06-01	唐登安	增加平台控制移除设备关联指令
2015-04-11	唐登安	增加设备 P2P 通信功能
2015-04-10	唐登安	1．重新定义 WIFI 终端获取组内列表， 2．增加 WIFI 终端通过平台转发数据至目标 WIFI 终端
2015-03-09	唐登安	增加手机端向服务器添加新的 WIFI 终端指令
2015-03-02	唐登安	增加通信网关与中心节点服务器通信指令（仅用于服务器平台间的通信）
2015-02-26	唐登安	增加获取当前设备的从设备指令
2015-02-25	唐登安	修改 CRC 校验高低位顺序
2015-02-12	唐登安	初始发布

通信协议

0xA0 链路操作

0x00 注册登录

长度(Byte)	名称	描述
n	设备密码	当前设备序号对应的密码 16 进制 MAC 地址(8Byte),按原顺存放，大端模式

回复格式:

长度(Byte)	名称	描述
n	通信令牌	服务器与当前设备通信的令牌

所有设备端收到的指令，都需要检查当前通信令牌是否匹配，如果不匹配，那么认为是非法服务器发来的指令，不予响应！

0x01 心跳数据包

数据区：无

0x55 设备点到点通信请求

请求数据报文：

长度(Byte)	名称	描述
8	目标通信设备	设备 ID

服务器应答报文(确认回复有以下字段，其它回复，没有以下字段):

长度(Byte)	名称	描述
8	目标通信设备	设备 ID
9	Torken	目标设备的 Torken,参看协议 Torken 配置
4	目标设备 IP	IP 地址（从左至右，大端）
2	目标设备 UDP 端口号	无符号 16 位，大端

0xEE 设备点到点通信确认（设备间）

数据报文：

长度(Byte)	名称	描述
8	发送设备 ID	设备 ID

指令中的设备 ID 为目标设备 ID，数据区中的为发送设备的 ID。

***P2P 建立流程：**

1．发起设备向服务器发送 0xA0 0x55；

2．服务器向双方设备通报对方的 IP，设备 ID，Torken 和 UDP 端口号；

3．设备向服务器发来的 UDP 端口号和 IP 地址发送 0xA0 0xEE，状态字节为：发送，一方收到后，即向对方当前 Socket 的 IP 和端口发送应答 0xA0 0xEE，状态字节为：确认，请注意，这个数据到达的 Socket 的 IP 和 端口不一定是服务器发来的。

4.当第一次通信建立成功后，即以不超过 1 分钟的频率，向对方发送 0xA0 0xEE 状态字节为：发送的数据包，以保持链路不被回收。

0xAA 数据传输

0x00 设备向平台获取组内设备

数据格式:

字段名	长度	描述
设备 ID	8	参看协议设备 id 定议
Torken	9	参看协议 torken 定议
IP	4	Ip 32,从左至右表示 IP(从左至右，大端)
PORT	2	无符号 16 位整型(大端)

0x55 设备通过平台向组内设备发送数据

数据格式:

字段名	长度	描述
设备 ID	8	参看协议设备 id 定议，接收设备的 ID
数据内容	N byte	要发送的数据内容

注：如果是发送：设备 ID 为接收设备的 ID,如果是接收数据：设备 ID 是发送设备 ID

0x66 设备点到点方式向组内已成功建立通信的目标设备发送数据

数据格式:

字段名	长度	描述
设备 ID	8	参看协议设备 id 定议，接收设备的 ID
数据内容	N byte	要发送的数据内容

注：设备 ID 为**发起数据发送**设备的 ID

0xAA 设备向平台透传 SOS 数据

消息体为透传的数据

0xEE 设备向平台透传数据

消息体为透传的数据

0xFF 平台向设备透传数据

消息体为透传的数据

***特别注意：使用此指令，设备 ID 必须替换成接收设备的 ID**

0xEF 平台或中心服务器与 APP 间的通信操作

0x00 登录[平台间]

中心服务器与网关服务器平台之间通信
数据格式及流程参见:0xA0 0x00

0x01 心跳[平台间]

中心服务器与网关服务器平台之间通信
数据格式参见:0xA0 0x01

0x06 添加新的 WIFI 终端[APP 与中心平台]

手机 APP 与中心服务器平台之间通信
参数区格式：

名称	描述
WIFI ID	8byte,见终端设备编码规则
WIFI 密码	8byte,见终端设备密码编码规则

0x07 移除已经关联的 WIFI 终端[APP 与中心平台]

手机 APP 与中心服务器平台之间通信
参数区格式：

名称	描述
WIFI ID	8byte,见终端设备编码规则

返回：成功，失败

0xF0 终端相关操作

0x07 设备请求从平台移除与用户关联

数据格式:

字段名	长度	描述
设备密码	8	参看设备密码定义

0x55 重启设备

数据区格式 ：无

0x56 服务器下发远程升级指令

1．服务器下发：
参数:

长度(Byte)	名称	描述
n	文件名	Gbk string
1	校验和	所有数据的校验和

2．设备向服务器请求文件

0x57 设备请求远程升级文件帧

长度(Byte)	名称	描述
n	文件名	Gbk string
2	帧序号	
2	帧大小	

0xA0 设备端执行 AT 指令

数据格式:

长度(Byte)	字段名	描述
n	AT 指令串	需要设备执行的 AT 指令串，详细定义见文档《Espressif AT 指令集》与《Ai-Thinker AT 指令集》。 设备执行完 AT 指令后，会返回 AT 指令执行结果字符串。

0xA1 设备端返回 AT 指令执行结果

数据格式:

长度(Byte)	名称	描述
n	AT 指令执行结果串	返回的 AT 指令执行结果。详细定义见文档《Espressif AT 指令集》与《Ai-Thinker AT 指令集》。 设备执行完 AT 指令后，会返回 AT 指令执行结果字符串。

0xA2 获取 GPIO 状态

数据格式:

长度(Byte)	名称	描述
1	GPIO 编号	需要获取状态的 GPIO 编号
1	GPIO 功能	0:关闭, 1:启动
1	GPIO 方向	0:INPUT, 1:OUTPUT

1	GPIO 电平	0:LOW, 1:HIGH
1	GPIO 中断	0:无, 1:低电平, 2:高电平, 3:上升沿, 4:下降沿, 5:双边

0xA3 设置 GPIO 状态

数据格式:

长度(Byte)	名称	描述
1	GPIO 编号	需要设置状态的 GPIO 编号
1	GPIO 功能	0:关闭, 1:启动
1	GPIO 方向	0:INPUT, 1:OUTPUT
1	GPIO 电平	0:LOW, 1:HIGH
1	GPIO 中断	0:无, 1:低电平, 2:高电平, 3:上升沿, 4:下降沿, 5:双边

0xA4 获取 PWM 状态

数据格式:

长度(Byte)	名称	描述
1	GPIO 编号	需要获取状态的 GPIO 编号
1	PWM 功能	0:关闭, 1:启动
2	PWM 频率	1~65535Hz.正常情况下 1000Hz.某些硬件不支持高频率。

2	PWM 占空比	0~1023

0xA5 设置 PWM 状态

数据格式:

长度(Byte)	名称	描述
1	GPIO 编号	需要设置状态的 GPIO 编号
1	PWM 功能	0:关闭, 1:启动
2	PWM 频率	1~65535Hz.正常情况下 1000Hz.某些硬件不支持高频率。
2	PWM 占空比	0~1023

0xA6 获取 ADC 状态

数据格式:

长度(Byte)	名称	描述
1	ADC 编号	ADC 通道编号，目前只支持 0x00（ADC0 电压）或 0x80（电源电压）
1	ADC 功能	0:关闭, 1:启动
2	ADC 数值	0~1023

0xA7 设置 ADC 状态

数据格式:

长度(Byte)	名称	描述
1	ADC 编号	ADC 通道编号，目前只支持 0x00（ADC0 电压）或 0x80（电源电压）
1	ADC 功能	0:关闭, 1:启动

0xAA 读取设备配置

参数:

长度(Byte)	名称	描述
1	参数 ID 低位	
1	参数 ID 高位	

参数对应表:

低位	高位	数据类型	对应参数描述	返回数据区格式
0x01	0x00	string	版本信息	String:“硬件版本”,”软件版本”,”Bootloader 版本”
0x05	0x00	Byte[]	通信服务器	2byte(低位在前)服务器端口 1byte 1:tcp 0:udp string:服务器 IP 或域名,以’\0’结束
0x06	**00**	**Byte[]**	**灾难服务器**	**2byte(低位在前)服务器端口** **1byte 1:tcp 0:udp** **string:服务器 IP 或域名,以’\0’结束** **(只有在通信服务器异常，不能正常登录时才登录此服务器，如果使用的是此服务器，需每隔 20 分钟查询一次通信服务器是否正常)**
0x07	0x00	Byte[]	通信服务器 DNS 配置	4byte:服务器 IP
0x0B	0x00	byte	数据发送等待时长	1byte
0x0C	0x00	byte	心跳包间隔	1byte,单位：秒
0x16	0x00	Byte[]	RTC	2byte 年 1byte 月 1byte 日 1byte 时

				1byte 分 1byte 秒 1byte 星期
0x20	0x00	byte	写超时	1byte
0x21	0x00	byte	读超时	1byte

0xAB 写设备配置

参数:

长度(Byte)	名称	描述
1	参数 ID 低位	
1	参数 ID 高位	
N	参数内容	

参看：**参数对应表**

0xF0 设备汇报状态事件

长度(Byte)	名称	描述

1	状态事件编码	见编码对应表
n	描述	Gbk string

0x10:设备升级状态
0x20:设备工作状态

0xFA 终端与 APP 内网通信

0xA0 设置 APP ID

本指令实现方式：
当手机 app 向服务器提交“添加新设备”成功后，向当前设备发送此指令
数据区格式:

长度(Byte)	名称	描述
8	APP ID	APP ID（8byte,小端）

设备收到后，需保存此 app id 至非易失存储器，下次内网通信时，app id 将作为 torken 包发送！

0xEE 设备向 APP 透传数据

消息体为透传的数据
***特别注意：**指令中的 torken 字段为 app id，只有收到 app 发来的内网通信，才能使用此指令回复 app,发往服务器是非法的。

0xFF APP 向设备透传数据

消息体为透传的数据

*特别注意：指令中的 torken 字段为 appid