|  |  |  |
| --- | --- | --- |
| C:\Users\king\Desktop\神州金山logo\1.png | **神州金山**  **技术文档** | 文件编号：SZJS-TEC-ZD-1708-001  页数：  版本： |

**物联网网关调试协议**

|  |  |  |  |
| --- | --- | --- | --- |
| 拟制 | 王中亚 | 日期 | 2017/9/5 |
| 评审 |  | 日期 |  |
| 批准 |  | 日期 |  |

**神州金山物联网科技（上海）有限公司**

|  |  |
| --- | --- |
| 以上信息解释权归神州金山所有 | 打印件及电子版不受控，同效力使用 |

**修订记录**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 日期 | 修订版本 | 编号 | 修改章节 | 修改内容 | 作者 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

目录

[目录 3](#_Toc501702892)

[1 适应范围 4](#_Toc501702893)

[2 系统名词 4](#_Toc501702894)

[3 通信方式 4](#_Toc501702895)

[4 报文格式 4](#_Toc501702896)

[4.1 报文格式 4](#_Toc501702897)

[4.1.1 起始域 5](#_Toc501702898)

[4.1.2 长度 5](#_Toc501702899)

[4.1.3 同步域 5](#_Toc501702900)

[4.1.4 消息头域 5](#_Toc501702901)

[4.1.4.1 消息id 5](#_Toc501702902)

[4.1.4.2 控制单元 6](#_Toc501702903)

[4.1.4.3 通信地址 6](#_Toc501702904)

[4.1.4.4 设备id 6](#_Toc501702905)

[4.1.4.5 终端id 7](#_Toc501702906)

[4.1.4.6 消息流水号 7](#_Toc501702907)

[4.1.4.7 时间标签 7](#_Toc501702908)

[4.1.5 数据域 7](#_Toc501702909)

[4.1.6 校验域 7](#_Toc501702910)

[4.1.7 结束域 7](#_Toc501702911)

[5 数据报文定义 8](#_Toc501702912)

[5.1 蓝牙查询指令 8](#_Toc501702913)

[5.1.1 查询设备信息（F001） 8](#_Toc501702914)

[5.1.2 心跳指令（0002） 9](#_Toc501702915)

[5.2 蓝牙操作设备指令 9](#_Toc501702916)

[5.2.1 重启指令（0003） 9](#_Toc501702917)

[5.2.2 查询火警历史记录 10](#_Toc501702918)

[5.3 文件操作指令 11](#_Toc501702919)

[5.3.1 请求下载文件指令（0F01） 11](#_Toc501702920)

[5.3.2 文件数据传输指令（0F02） 11](#_Toc501702921)

[5.3.3 文件传输完成指令（0F03） 12](#_Toc501702922)

[6 附录 13](#_Toc501702923)

[6.1 设备id 13](#_Toc501702924)

[6.2 终端id 13](#_Toc501702925)

[6.3 火警类型 14](#_Toc501702926)

# 适应范围

本协议适应于神州金山物联网与消防监控平台之间的通信。

本协议适应于消防监控设备与监控平台之间的通信。

本协议适应于消防监控设备RS485接口的通信。

# 系统名词

SVR：中心服务器（监控平台）

GW：物联网网关

DEV：监控设备

# 通信方式

# 报文格式

## 报文格式

一条报文包括：起始域、长度域、同步域、消息头域、数据域、校验域和结束域。

|  |  |  |
| --- | --- | --- |
| 字段名 | 长度 | 说明 |
| 起始域 | 1byte | 0x3A |
| 长度 | 2byte | 地址域~用户数据。2个字节，低字节在前 |
| 同步域 | 1byte | 0x3A |
| 消息头域 | 4byte |  |
| 数据域 | Nbyte |  |
| 校验域 | 2byte | CRC16 |
| 结束域 | 1byte | 0x16 |

### 起始域

0x3A

### 长度

长度用两个字节表示，指的是地址与、控制单元、设备类型、命令字、数据域、时间戳的长度。

一条报文的总长度=LEN+4。

* 注意：指令的长度最大不超过256bytes。

### 同步域

同步域为1个字节，为0x3A

### 消息头域

|  |  |  |
| --- | --- | --- |
| 字段名 | 长度 | 说明 |
| 命令id | 2byte |  |
| 控制单元 | 2byte |  |
| 通信地址 | 4byte | 地址域~用户数据。2个字节，低字节在前 |
| 设备id | 2byte |  |
| 终端id | 2byte |  |
| 消息流水号 | 2byte | 预留 |
| 时间标签 |  |  |

#### 消息id

消息id标示该条指令的用处。2个字节（低字节在前高字节在后）。

|  |  |
| --- | --- |
| CMD | |
| CMDL | CMDH |

#### 控制单元

控制单元为2个字节，由AFN和FLAG两部分组成。

AFN标示了一条报文的功能大类。详细的AFN定义分配参考章节5。

控制单元FLAG标示了数据的标示，定义如下：

控制单元属性格式

低八位

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| BIT7 | BIT6 | BIT5 | BIT4 | BIT3 | BIT2 | BIT1 | BIT0 |
| - | - | - | - |  | TIM | M/S | U/D |

高八位

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| BIT15 | BIT14 | BIT13 | BIT12 | BIT11 | BIT10 | BIT9 | BIT8 |
| - | - | - | - |  |  |  |  |

U/D：数据上下行标志，0：下行（Server->Client） 1:上行（Client->Server）

* M/S：设备主从标志。0：主设备（报文发起方） 1：从设备（报文接收方）
* TIM：时间标志。该设备只能由主设备置位，如果该位被置位，则报文必须带有时间，如果该位未置位，则报文无时间。

#### 通信地址

通信地址为4个字节，预留。

#### 设备id

用于标识设备的类型，2个字节（低字节在前高字节灾后）。

|  |  |  |
| --- | --- | --- |
| 设备类型符 | 说明 | 备注 |
| 0x0100 | 网关 |  |
|  |  |  |
| 0xFF | 当设备id为0xFF的时候，该设备下面无终端（终端id为0xFF），直接和平台通信。 |  |

**注：当该设备下面无终端的时候，设备id为0xFF，并且终端id也为0xFF。**

#### 终端id

用于标识设备的类型，2个字节（低字节在前高字节灾后）。

|  |  |  |
| --- | --- | --- |
| 设备类型符 | 说明 | 备注 |
| 0x0100 | 烟雾火灾 |  |
| 0x0200 | 手动报警 |  |
|  |  |  |
| 0xFF |  |  |

#### 消息流水号

1. 对于消息流水号，其值从0开始，没发送一套消息后，消息流水号增加1.超过65535重新从0开始

#### 时间标签

时间标签用于存放报文的时间，有年、月、日、时、分、秒组成。

### 数据域

数据域用于存放报文的数据，受报文的总长度限制。

### 校验域

用于校验数据长度域的数据长度校验。包括地址域、控制单元、设备类型、命令字、数据域、时间戳，校验采用crc16。

### 结束域

0x16标识一条报文的结束。

# 数据报文定义

## 蓝牙查询指令

### 查询设备信息（F001）

指令说明：该指令由app发起，在手机蓝牙连接上GW以后发起，用于查询设备的一些：

【DEV -> SVR】：68 [LL] [SYNC] {[CMD] [ADDR] [CU] [DEV] [NODE] [MES] [DT]} {[para1] [para2] [para3] [para4] [para5]} [CRC] 16

》[CMD] = 01 00H

》[CU] 2字节，控制单元。数据为B0为1；TIM为0；

》[ADDR] 4字节，预留；数据为：00 00 00 00 。

》[DEV] 2字节，设备的id；如：00 01位物联网网关

》[NODE] 2字节，终端的id，登录包该值为 00 00

》[MES] 2字节，消息流水号好，预留用，全部为 00 00

》[DT] 6字节，日期。

》[para1] 6字节，GW的ID；如：AA AB AC 4A 55 AF。（）

》[para2] 2字节，当前GW的软件版本号，主板号在前；

如：0201表示02.01版本。

》[para3] 6字节，当前硬件编号，如：30 20 00 01

》[para4] 6字节，MAC地址，如：AA AB AC 4A 55 AF

》[para5] 8字节，GSM模块的IMEI识别码，无法获取时为 FF FF FF FF FF FF FF FF

如：IMEI=123456789012345时[para5]=01 23 45 67 89 01 23 45

**注：其中[para4] [para5]针对不同的设备，可以没有；是可选参数。**

【SVR -> DEV】：68 [LL] [SYNC] {[CMD] [ADDR] [CU] [DEV] [NODE] [MES] [DT]} {[data1] } [CRC] 16

》[CMD] = 01 00H

》[data1] 1字节，登录结果

1. 成功
2. 错误

### 心跳指令（0002）

指令说明：该指令由GW发起，登录成功后，如果服务器为和GW通信，则GW每隔一定时间发起一次心跳，保持和服务器的连接；如果服务器和GW一直在通信，GW不发起心跳包。

【DEV -> SVR】：68 [LL] [SYNC] {[CMD] [ADDR] [CU] [DEV] [NODE] [MES] [DT]} {[para1] } [CRC] 16

》[CMD] = 02 00H

》[para1] 6字节，GW的ID；如：AA AB AC 4A 55 AF。

**注：[para1] 是可选参数。**

【SVR -> DEV】：68 [LL] [SYNC] {[CMD] [ADDR] [CU] [DEV] [NODE] [MES] [DT]} {[data1]} [CRC] 16

》[CMD] = 02 00H

》[data1] 6个字节，为收到[para1]的数据。

**注：如果GW连续三次发送心跳包都未能收到服务器的回应时，GW重新连接服务器；其中[data1]为可选参数。**

## 蓝牙操作设备指令

### 重启指令（0003）

指令说明：该指令由服务器发起，让GW重启，GW收到指令后立即执行。

【SVR -> DEV】：68 [LL] [SYNC] {[CMD] [ADDR] [CU] [DEV] [NODE] [MES] [DT] } {[para1]} [CRC] 16

》[CMD] = 03 00H

》[para1] 1字节，重启模式：

1. 初始化重启，设备恢复出厂设置
2. 一般重启，保持当前数据并重启

【DEV -> SVR】：68 [LL] [SYCN] {[CMD] [ADDR] [CU] [DEV] [NODE] [MES] [DT] } {} [CRC] 16

》[CMD] = 03 00H

### 查询火警历史记录

指令说明：该指令由手机APP发起，用于查询网关中火警记录。

【DEV -> SVR】：68 [LL] [SYNC] {[CMD] [ADDR] [CU] [DEV] [NODE] [MES] [DT] } {[para1] [para2] [para3] [para4] [para5] [para6] [para7] [para8]} [CRC] 16

》[CMD] = 01 01H   
》[para1] 2个字节，火警信息包序号

》[para1] 2个字节，上传火警信息记录的条数;为N就是有N条火警记录

》[para1] 2个字节，火警记录编号；第一条记录为1

》[para1] 4个字节，楼号；预留

》[para2] 4个字节，区号

》[para3] 4个字节，回路号

》[para4] 4个字节，点位号

》[para5] 1个字节，表示火警状态

00 无火警

01 火警

02 测试火警

》[para1] 2个字节，火警记录编号；第二条记录为2

》[para1] 4个字节，楼号；预留

》[para2] 4个字节，区号

》[para3] 4个字节，回路号

》[para4] 4个字节，点位号

》[para5] 1个字节，表示火警状态

00 无火警

01 火警

02 测试火警

【DEV -> SVR】：68 [LL] [SYCN] {[CMD] [ADDR] [CU] [DEV] [NODE] [MES] [DT]} {} [CRC]

## 文件操作指令

### 请求下载文件指令（0F01）

指令说明：由服务器发起，通知GW，准备接收文件。

【SVR -> DEV】：68 [LL] [SYNC] {[CMD] [ADDR] [CU] [DEV] [NODE] [MES] [DT] ]} {[para1] [para2] [para3] } [CRC] 16

》[CMD] = 01 0FH

》[para1] 1个字节，操作类型

00 表示退出文件传输模式

01 表示进入文件模式，开始重新传输模式

02 表示继续上一次的文件操作

》[para2] 100个字节，表示要升级的文件名； 如：文件名为ww123.txt最高位为w最低位为t

》[para3] 32个字节，文件校验值；采用MD5校验算法；

**注：文件名不能使用汉字**

【DEV -> SVR】：68 [LL] [SYNC] {[CMD] [ADDR] [CU] [DEV] [NODE] [MES] [DT] ]} {[data1] [data2]} [CRC] 16

》[CMD] = 01 0FH

》[para1] 1个字节，

### 文件数据传输指令（0F02）

指令说明：用户传输文件，服务器发送一个数据包GW接收一个数据包。

【SVR -> DEV】：68 [LL] [SYNC] {[CMD] [ADDR] [CU] [DEV] [NODE] [MES] [DT]} {[para1] [para2] [para3] [para4]} [CRC] 16

》[CMD] = 02 0FH

》[para1] 4个字节，文件数据包总个数；高位在前；如；00 00 32 22

》[para2] 4个字节，文件数据包传输的序号；高位在前；如00 00 00 01表示第一个包。

》[para3] 2个字节，文件数据包的长度n；一般设定512bytes；

》[para4] n个字节，文件数据包数据；

**注：最后一包数据长度不足512个字节的时候，[para3]按实际数据包填写。**

【DEV -> SVR】：68 [LL] [SYNC] {[CMD] [ADDR] [CU] [DEV] [NODE] [MES] [DT] } {[data1] [data2] [data3]} [CRC] 16

》[CMD] = 02 0FH

》[data1] 4个字节，文件数据包总个数；高位在前；如；00 00 32 22

》[data2] 4个字节，文件数据包传输的序号；高位在前；如00 00 00 01表示第一个包。

》[data3] 1个字节，操作结果；

00 表示成功

01 表示该数据包出错

### 文件传输完成指令（0F03）

指令说明：文件传输完成后，校验数据的完整性。

【SVR -> DEV】：68 [LL] [SYNC] {[CMD] [ADDR] [CU] [DEV] [NODE] [MES] [DT]} {[para1]} [CRC] 16

》[CMD] = 03 0FH

》[para1] 32个字节，文件校验值；采用MD5校验算法；

【DEV -> SVR】：68 [LL] [SYNC] {[CMD] [ADDR] [CU] [DEV] [NODE] [MES] [DT]} {[data1]} [CRC] 16

》[CMD] = 02 0FH

》[data1] 1个字节，操作类型

00 文件完整

01 文件错误

# 附录

## 设备id

## 终端id

## 火警类型

|  |  |  |
| --- | --- | --- |
| 火警类型值 | 火警类型 | 说明 |
| 00 | 通用 |  |
| 01 | 烟感 |  |
| 02 | 手报 |  |
|  |  |  |
|  |  |  |
|  |  |  |