通讯数据帧头格式定义V3

# 文档变更记录

|  |  |  |  |
| --- | --- | --- | --- |
| 版本号 | 日期 | 作者 | 说明 |
| 1.0 | 2014-10-01 | 范小雨 | 初稿 |
| 1.1 | 2015-04-26 | 范小雨 | 1. 平台通讯的GUID不在数据头内传输 |
| 3.0 | 2015-09-13 | 范小雨 | 1. 修改帧描述内容 |
| 3.0 | 2015-11-11 | 范小雨 | 1. 修改SessionID描述 2. 修改通讯帧封装说明的错误 |
| 3.1 | 2016-06-27 | 穆青 | 1、 增加对帧序号的详细描述  2、 增加将时间戳加入数据帧合法性运算的描述  3、 增加平台代理转发提取设备MAC说明  4、 去掉短数据头的定义  5、 增加代理转发头中GUID生成描述。 |

# 协议分层

局域网服务端口号：UDP端口：1066

应用协议分为三层：帧头、数据头、数据

|  |
| --- |
| 帧头 |
| 数据头 |
| 数据 |

## 帧头格式：

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 控制终端和平台通讯与网关或WIFI设备通讯：帧头格式8+16+8字节） | | | | | | | | |
|  | Bit7 | Bit6 | Bit5 | Bit4 | Bit3 | Bit2 | Bit1 | Bit0 |
| 帧头 | FIN | MASK | Ver | | Short | Opcode | | |
| 保留字 | 1 字节 | | | | | | | |
| 帧序号 | 2 字节 | | | | | | | |
| 时间戳 | 4 字节 | | | | | | | |
|  | 长帧扩展数据（源、目的ID） | | | | | | | |
| 目的地址 | 8 字节 | | | | | | | |
| 源地址 | 8 字节 | | | | | | | |
|  | 转发帧扩展数据（GUID代理转发时使用） | | | | | | | |
| GUID | 16 字节 | | | | | | | |

1. 基础帧内容说明：

* 基础帧内容：帧头字节、保留字、包序号、时间戳。
* 帧头：帧头字节1。

FIN：标识数据包是否是最后一包，0-不是；1-最后一包数据。

MASK：隐藏加密帧头数据，0-不隐藏；1-隐藏。加密从时间戳以后的帧头+数据头，如果是代理转发帧头只隐藏源地址、目的地址和GUID。

Ver：帧头数据格式版本号。

Short：帧头和数据头类型，0：长帧、数据头类型；1：短帧、数据头类型。

Opcode：操作识别码。

0：控制终端与设备终端局域网通讯数据。

1: 控制终端与设备终端广域网直接通讯数据。

2：终端设备与平台通讯数据。

3：终端设备需要平台代理转发数据。

4：手机使用6LowPAN直接控制设备的帧类型，使用短帧、数据头。

5：设备发送数据到设备（联动时用）的帧类型，使用长帧、数据头。

0x6-0x7：保留。

* 保留字：预留字节，值为0；
* 帧序号：针对当前会话帧序号计数，主动发送帧，每发出一帧序号加1，接收端每接到一帧数据对比是否小于等于上一帧号，如果是，则丢弃；对于回复帧，直接采用发送帧的帧序号作为当前回复帧的帧序号，发送方接收到回复帧后判断帧序号是否与自己发送的帧序号一致，不一致则丢弃，用来防止路由重复发生UDP数据包问题；当客户端判断到自己主动发送的或者服务端主动发送的包序号大于65000的时候则强制重新登录服务端，登录帧的包序号从0开始累加。
* 时间戳：毫秒级数值，回应方使用收到发送方的时间戳回应。

1. 长帧扩展内容：

目的地址：指令到达的目标设备地址或ID号。

源地址：指令发出的源设备ID号码。手机端如果有用户登录必须使用用户ID，如果没有就用手机MAC做源ID。

1. 转发帧扩展内容：

GUID：与平台会话ID，在代理转发帧头时使用，数据组成是从平台会话回复包取8字节guid，拼接8个0，AES私钥加密后共16字节。

1. 针对opcode=3的转发帧MAC提取说明：

鉴于子设备可以通过任意网关会话与平台通讯，平台不应提取转发帧头内的源ID作为 用户的绑定关系判断，应该从转发帧下面的opcode=1的帧头中提取源ID与目的ID来 判断设备与用户之间的绑定关系。

## 数据头格式：

1. 数据头格式：

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 数据头格式（10字节） | | | | | | | | | | | | |
|  | Bit7 | | Bit6 | | Bit5 | Bit4 | | Bit3 | Bit2 | | Bit1 | Bit0 |
| Flags | Read | ACK | | DataFormat | | | KeyLevel | | | EncryptType | | |
| Data seuq | Data Sequence 8位 | | | | | | | | | | | |
| MsgID | 16位 | | | | | | | | | | | |
| Lenght | 16位 | | | | | | | | | | | |
| HeadCheck | 8位 | | | | | | | | | | | |
| Check | 8位 | | | | | | | | | | | |
| Session id | 16位，平台会话为64位 | | | | | | | | | | | |
| Data | ……… | | | | | | | | | | | |

1. 数据头内容说明：

Flags：

Read：表示当前消息ID是读取还是写入，0-写入；1-读取

DataFormat：数据格式。

0x0：二进制数据格式。

0x1：JSON格式数据。

0x2：XML格式数据。

KeyLevel：密钥级别；

1. 不加密。
2. 随机密钥。
3. 登录成功后运算的密钥。
4. 随机密钥+登录成功后运算的密钥。

EncryptType：加密类型，0-RC4算法，1-DES加密，2-AES128加密。

Data seuq：数据包序号和，与消息ID对应的数据每更新一次序号加1，用来判断接收端是否收到最新数据内容。

MsgID：消息ID号，详细见消息类型定义

Length：表示包含数据长度。

HeadCheck：帧头和数据头校验值，校验长度从帧头开始到数据长度字段（包含数据长度）；校验算法为8位CRC运算。

Check：数据校验值，校验长度从Session id开始到数据结尾；校验算法为8位CRC运算。

Session id：登录成功后返回的ID，用来检验数据来源的合法性，当发送数据到平台时为8字节长度。

Data：对应MsgID的相关数据，具体数据格式参阅不同设备的数据格式定义文档。

# 帧序号使用说明：

为了防止通讯造成数据重复问题，在帧头增加帧序号校验；需要记录自己发出的帧序号和对方发送的帧序号；自己发出数据要将自己帧序号+1，接收对方数据后要校验对方帧序号，如果接收到的帧序号小于或等于记录的帧序号，且对方帧序号没有到最大反转值的情况下，丢弃此帧数据。

**注：每个会话都应有独立的帧序号变量**



# 时间戳使用说明：

32位毫秒级数值；主动发送方在封装帧内容时，获取本地毫秒级时间戳给帧时间戳赋值；接收方回应发送方此帧数据时，帧头时间戳使用发送方的时间戳数值回应；可以用来测试通讯延时。



# 数据序号使用说明：

协议已经定义回应数据收到指令，但在实际运行过程中，往往状态数据改变速度大于网络通讯的速度，这就导致状态其中一端不能收到最后一次状态数据；一次我们定义了数据序号（取值0～255）

**注：每个指令数据类型都应有独立的数据序号变量**



# 通讯帧封装说明：

1. 局域网控制终端与设备通讯帧描述：

控制终端与设备在家庭局域网通讯时使用此帧头、数据头封装格式进行通讯。



1. 广域网手机与设备通讯帧描述：

控制终端与设备在广域网通讯或通过平台转发时使用此帧头、数据头封装格式进行通讯。



1. 设备与云平台通讯帧描述：

设备与云平台进行通讯时使用此帧头、数据头封装格式进行通讯。



1. 手机与设备通讯通过平台转发帧描述：

手机与设备进行远程通讯，通过平台转发时的帧封装格式；平台会话ID在传输时必须加密传输，转发头后面“广域网手机与设备通讯帧内容”不参与行平台会话加密。



1. 手机直接使用6LowPAN控制设备帧描述：

当具有6LowPAN直控设备功能手机与6LowPAN设备通讯时使用此帧头、数据头封装格式。



1. 设备与设备通讯帧描述：

当设备与设备进行联动通讯时使用此帧头、数据头封装格式。



1. 设备与网关通讯帧格式：

当6LowPAN设备与网关设备进行交互或通过网关转发数据时，使用此帧头、数据头封装格式；局域网与手机通讯的操作识别码为0，向平台发送数据为3。

