

**2.4G通信协议**

**版本号V001R005**

**概要设计文档**

**深圳市银河风云网络系统股份有限公司**

**Shenzhen GALAXYWIND Network Systems Co., Ltd.**

地址：深圳市高新技术产业园区北区新西路5号银河风云大厦

Address: GALAXYWIND building, No.5 Xinxi road, Shenzhen High-Tech Industry Park, NanShan district, China

邮编 P.C.: 518055

电话 Tel: +86-755-83400088

传真 FAX: +86-755-86139063

网站 Web: http://[www.galaxywind.com](http://www.galaxywind.com)

客服 Hotline: 4000009879

企业QQ: 4000009879

微信公众号 WeChat:



**版权声明**

版权所有©深圳市银河风云网络系统股份有限公司2015。深圳市银河风云网络系统股份有限公司（以下简称"银河风云"）对本资料进行版权声明，未经银河风云书面许可，任何单位及个人不得以任何方式或理由对本资料的任何内容进行复制、修改、抄录、传播。

**商标声明**

"银河风云"，"GALAXYWIND"等是深圳市风云实业有限公司的注册商标，本文档提及的其他商标、服务标志、注册商标及注册服务标志均为其所有者拥有。

**免责声明**

本资料会进行不定期更新，本资料中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目录

[1 介绍 4](#_Toc436396601)

[1.1 总体结构 4](#_Toc436396602)

[1.2 使用流程 5](#_Toc436396603)

[1.3 简化版设备端 6](#_Toc436396604)

[1.4 网关、设备类型定义 7](#_Toc436396605)

[1.5 UDP通信协议 7](#_Toc436396606)

[1.5.1 IA.RFGW.JOIN 7](#_Toc436396607)

[1.5.2 IA.RFGW.JOIN\_FIND 8](#_Toc436396608)

[1.5.3 IA.RFGW.JOIN\_ACTION 8](#_Toc436396609)

[1.5.4 IA.RFGW.PARAM 8](#_Toc436396610)

[1.5.5 IA.RFGW.GROUP 8](#_Toc436396611)

[1.5.6 IA.RFGW.LIST 9](#_Toc436396612)

[1.5.7 IA.RFGW.LIST\_DIGEST 10](#_Toc436396613)

[1.5.8 IA.RFGW.LIST\_DIGEST\_ACK 10](#_Toc436396614)

[1.5.9 IA.RFGW.LIST\_WITH\_ID 10](#_Toc436396615)

[1.5.10 IA.RFGW.TT 11](#_Toc436396616)

[1.5.11 IA.RFGW.TT\_CACHE 11](#_Toc436396617)

[1.5.12 IA.RFGW.DEV\_SYNC 12](#_Toc436396618)

[1.5.13 IA.RFGW.DEV\_GROUP 12](#_Toc436396619)

[1.5.14 IA.RFGW.DEV\_GROUP\_MEMBER 12](#_Toc436396620)

[1.5.15 IA.RFGW.DEV\_GROUP\_TT 13](#_Toc436396621)

[1.5.16 IA.RFGW.DEV\_NANE 13](#_Toc436396622)

[1.6 UDP通信协议常量定义 13](#_Toc436396623)

[1.7 RF通信协议 14](#_Toc436396624)

[1.7.1 申请配对 14](#_Toc436396625)

[1.7.2 允许配对 15](#_Toc436396626)

[1.7.3 下发配对 15](#_Toc436396627)

[1.7.4 认证请求 15](#_Toc436396628)

[1.7.5 认证提问 15](#_Toc436396629)

[1.7.6 认证答案 16](#_Toc436396630)

[1.7.7 认证结果 16](#_Toc436396631)

[1.7.8 保活和命令下发 16](#_Toc436396632)

[1.7.9 Beacon 17](#_Toc436396633)

[1.7.10 保活报文 17](#_Toc436396634)

[1.7.11 网关向设备主动发送保活询问是否在线 17](#_Toc436396635)

[1.7.12 网关向设备发送透传命令 18](#_Toc436396636)

[1.7.13 设备向网关发送透传应答 18](#_Toc436396637)

[1.7.14 网关向设备发送透传命令获取通用缓存 18](#_Toc436396638)

[1.7.15 设备向网关发送透传应答发送通用缓存 18](#_Toc436396639)

[1.7.16 推送透传请求,缓存 19](#_Toc436396640)

[1.7.17 推送透传应答，缓存 19](#_Toc436396641)

[1.7.18 推送透传请求 19](#_Toc436396642)

[1.7.19 推送透传应答 19](#_Toc436396643)

[1.7.20 网关向设备发送消息 19](#_Toc436396644)

[1.7.21 设备向网关发送应答 20](#_Toc436396645)

[1.7.22 推送请求 20](#_Toc436396646)

[1.7.23 推送应答 20](#_Toc436396647)

[1.7.24 组播透传请求 20](#_Toc436396648)

[1.7.25 RF信号干扰解决 21](#_Toc436396649)

[1.7.26 信道占用指示报文 21](#_Toc436396650)

[1.7.27 升级协议 21](#_Toc436396651)

[1.8 网关设计 22](#_Toc436396652)

[1.8.1 设备数据结构 22](#_Toc436396653)

[1.8.2 发送队列 23](#_Toc436396654)

[1.8.3 接收队列 23](#_Toc436396655)

前言

**概述**

基于2.4G实现的通信系统的协议设计。

**产品版本**

与本文档相对应的产品版本如下所示：

|  |  |
| --- | --- |
| **产品名称** | **产品版本** |
| 2.4G通信协议概要设计 | 1.0 |

**阅读对象**

本文档主要适用于以下用户：

结构设计工程师【√】

硬件开发工程师【√】

软件开发工程师【√】

系统规划工程师【√】

系统维护工程师【√】

**约定**

**符号约定**

文档中可能出现的符号定义如下所示：

|  |  |
| --- | --- |
| **符号** | **说明** |
| 警告警告 | 表示有中度或低度潜在危险，如果不能避免，可能导致较严重结果。 |
| 注意注意 | 表示有潜在风险，如果忽视这些文本，可能导致不可预知的结果。 |
| 备注备注 | 表示对正文的强调和补充。 |

**通用格式约定**

|  |  |
| --- | --- |
| **格式** | **说明** |
| 黑体 | 中文：1 -6级标题，图表/表格标题采用黑体 |
| Arial | 英文：1 -6级标题，图表/表格标题采用Arial |
| 宋体 | 中文：正文采用宋体 |
| Times New Roman | 英文：正文采用Times New Roman |

**修改记录**

|  |  |  |  |
| --- | --- | --- | --- |
| **修订时间** | **修订人** | **审核人** | **修订版本** |
| 2015-3-25 | 陈文辉 |  | 1.0 |
| 2015-4-17 | 陈仕建 |  | 1.1 |
| 2015-4-24 | 谭洪国 |  | 1.2 |
| 2015-7-15 | 陈仕建 |  | 1.3  1、增加简化版设备  2、增加设备端流程图  3、修改绑定解绑方式  4、设备分组及RF组播批量控制  5、给设备改名字  6、RF载荷第一字节最高位作为加密标志 |
| 2015-10-30 | 谭洪国 |  | 1.4  增加rf冲突避让机制  增加app设置网关兼容模式 |
| 2015-11-16 | 谭洪国 |  | 1.5  增加UDP优化通信量协议 |

# 介绍

本文主要描述RF网关、RF设备的组网结构和通信协议。本文RF网关可以简称网关，RF设备简称设备。

## 总体结构

为实现大规模(最多128个设备)、低价格、低功耗（设备端）组网方案，在现有UDP设备基础上，把现有UDP设备拆分成RF网关和RF设备两部分，组网拓扑入下图所示：

UDP

我家网关2

我家网关1

服务器

手机

UDP UDP

2.4G 2.4G 2.4G

设备3

设备2

设备1

这里的设备可以是单片机直接驱动电器（如插座，灯），也可以是带有单片机的电器（与第三方合作），通过串口与我们的单片机对接。

为了便于用户批量控制，可以对设备进行分组，分组信息存放在网关。一台设备可以属于多个分组。

## 使用流程

手机通过服务器或局域网连接到网关，从网关查询设备列表，根据设备的类型显示相应的控制界面。为避免网关代码量过大，手机对设备的控制采用透传方式。

设备和网关要绑定后才能使用

* 绑定：

新设备轮训各个信道发送绑定（配对）申请并等待一定时间（如2秒）响应，网关把新设备作为未绑定设备推送给手机app，app在醒目位置提示用户发现新设备，用户可以确认绑定或拒绝绑定。如果存在多个网关在线，以最先确认绑定的为准。

* 解绑

已绑定设备可能需要解绑（如更换网关），解绑分为安全性和高安全性两种情况

1、低安全性

例如灯，没有按钮可以操作，这类设备在一定时间内无法连接到已经绑定的网关，进入绑定流程尝试绑定到其它网关。在连接旧网关和绑定新网关反复切换直到连接到网关。

为了避免自家网关出故障情况下，邻居家出现一大堆新设备，设备端发送绑定申请时带上是否已经绑定过标志。网关推送给手机app时，也带上此标志。如果已经绑定过，app在本地缓存查找是否有该设备，如果有，直接回复允许绑定给网关，网关完成绑定。如果没有缓存，用户需要操作app的“找回旧设备”按钮，才能看见这些设备，然后用户可以“允许绑定”或“拒绝绑定”。这样用户只有在同时换网关和手机情况下，下需要“找回旧设备”。

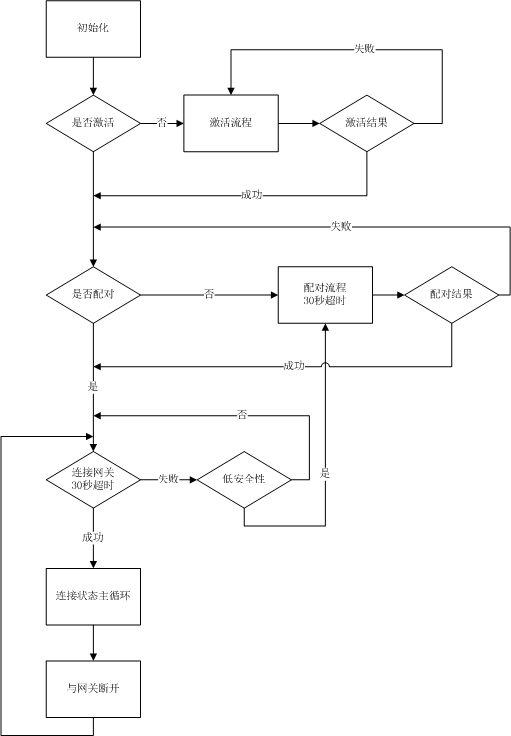
2、高安全性

例如门锁，有按钮可以操作，用户按下按钮后清除绑定信息，重新进入绑定流程。

两种解绑方式由编译宏控制，不同产品可以选择不同的解绑方式。

对于一个用户有多个网关情况，手机添加多个网关并登录后，可以把多个网关划分成漫游组，组内网关会同步各自的设备信息，这样设备移动后可以接入组内任意网关。

设备端软件流程总体图如下：



## 简化版设备端

由于标准版协议复杂，对单片机资源要求较高，在低端产品无成本优势，需要开发出基于51系列单片机的低成本简化版RF设备。简化版需求如下：

* 绑定、解绑

与标准版相同

* 认证

与标准版相同

* 不支持升级
* 不实现RF时隙协议

简化版单片机资源有限，不实现完整的RF时隙协议，单片机和RF芯片不考虑节电，不休眠。

接收：

RF长期处于RX状态，只有在需要发送数据时切换到TX状态，发送完成立即切换回RX状态。

发送：

设备收到网关下发命令后，延时到回应ACK的时隙发送ACK给网关。

需要主动上报数据时，根据上次收到Beacon帧时间延时到竞争上报时隙发送给网关。

* 支持单播和组播方式控制设备端

设备端同时可以接收单播和组播控制命令。

* 单片机资源预算

Flash：8KB，RAM：512B

## 网关、设备类型定义

网关类似于悟空，子类型定义为IJ\_RFGW=0x1E，采用6621模组的网关扩展类型定义为ETYPE\_RFGW\_6621=0x01

直接驱动电器的设备，设备子类型和扩展类型在激活时确定。

通过单片机对接驱动电器的设备，参考联创的透传协议，一般要求我们的设备通用，电器上的单片机上报电器类型给我们的设备，手机app以此来判断设备扩展类型。

## UDP通信协议

RF网关UDP通信协放在IA对象下面，子对象RFGW

//IA.RFGW

#define UCSOT\_IA\_RFGW 21

### IA.RFGW.JOIN

UCAT\_IA\_RFGW\_JOIN（废弃）

手机指示网关进入配对模式，只支持set操作，报文格式为：

|  |  |  |  |
| --- | --- | --- | --- |
| 0 | 1 | 2 | 3 |
| TimeOut | | Reserved | |

TimeOut：网关进入配对模式时间长度，单位秒，超时还没有设备上了，恢复正常模式。

### IA.RFGW.JOIN\_FIND

UCAT\_IA\_RFGW\_JOIN\_FIND（废弃）

网关上报配对时新发现的设备，只支持push操作，报文格式为：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 0 | | 1 | 2 | 3 |
| Dev sn | | | | |
| Dev SubType | Dev ExType | | Reserved | |

### IA.RFGW.JOIN\_ACTION

UCAT\_IA\_RFGW\_JOIN\_ACTION

手机指示网关配对新发现的设备进行确认，只支持set操作，报文格式为：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 0 | | 1 | 2 | 3 |
| Dev sn | | | | |
| Accept | Reserved | | | |

Accept：1表示同意设备接入，0表示拒绝设备入网

### IA.RFGW.PARAM

UCAT\_IA\_RFGW\_PARAM

手机配置网关参数，只支持get，set，push操作，报文格式为：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 0 | | 1 | | 2 | 3 |
| Compat | Channel | | is\_upgrade | | Reserve |
| Reserve | | | | | |
| Reserve | | | | | |
| Reserve | | | | | |
| Reserve | | | | | |
| Reserve | | | | | |
| Reserve | | | | | |
| Reserve | | | | | |

Compat：0默认兼容级别；1~255，兼容级别，数字越大，越不兼容老版本，而使用新特性。

Channel：0默认信道；1~255为信道号，2400+信道号为网关使用频率。

is\_upgrade:0没有升级中，1在升级中

Reserve：保留其他参数用。

### IA.RFGW.GROUP

UCAT\_IA\_RFGW\_GROUP

手机给网关配置漫游组，只支持get、set操作，报文格式为：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 0 | | 1 | 2 | 3 |
| PSK（8字节） | | | | |
| RFGW-Count | Reserved | | | |
| RFGW1 sn | | | | |
| RFGW2 sn | | | | |
| ...... | | | | |

PSK：网关漫游组预共享秘钥

RFGW-Count：网关数量

考虑到用户更换手机或重装app，手机登录网关后，先要get漫游组信息（相同PSK的网关认为同组），如果网关还没有划分到漫游组，get响应报文PSK和RFGW-Count都填0。

### IA.RFGW.LIST

UCAT\_IA\_RFGW\_LIST

网关当前在线设备列表，支持set、delete、get、push操作，报文格式为：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | | | 3 |
| Dev-count | Totle-count | Reserved | | | |
| Dev1 sn | | | | | |
| Dev1 SubType | Dev1 ExType | | flags | TLV\_count | |
| TLV... | | | | | |
| .......(Next Dev) | | | | | |

flags:

bit0表示设备是否在线（1表示在线）

bit1 表示是否是新设备（1表示新设备）

bit2 表示设备正在绑定

bit3-bit7保留

手机get请求Dev-count填0，网关回应填具体设备个数

手机delete请求可以删除已经配对的设备

手机set请求主要用来给设备取个名字。由于2.4G RF通信只能传很少字节，设备名字就只保存在网关上。

由于设备可能名字比较长，为避免ip分片，当设备数量较多时，需要应用层把设备列表切割成多个报文传输。

TLV包含设备的一些属性，例如：

UCT\_VENDOR 设备vendor-id

UCT\_NAME 设备名称

UCT\_ETYPE 设备扩展类型（字符串）

UCT\_VERSION 设备版本

UCT\_PSK 设备共享秘钥（网关发给手机不包含pks，网关之间同步设备信息包含）

优化UDP协议：

1、网关增加设备统一状态缓存，透传用TT\_CACHE命令，旧设备或手机任然使用TT，新手机登录网关是协商得知网关是否有支持TT\_CACHE能力

2、手机缓存设备列表及设备列表摘要。登录时查询一次摘要，再根据摘要变化可靠查询相应设备。

3、网关在设备列表信息变化时，推送摘要到手机，手机根据摘要变化可靠查询相应设备。

4、设备状态变化，推送到网关，网关更新缓存，再构造临时报文发送到手机，设置发送中标志，收到响应后清除标志，否则超时重新构造临时报文重发。

5、网关增加发送不可靠报文方法，来实现3、4点，构造临时报文发送后设置标志，设置发送中标志，收到响应后清除标志，否则超时重新构造临时报文重发。

6.网关收到列表摘要请求，认为手机支持列表摘要推送，不再推送完整列表。否则推送完整列表。新网关有有TT\_CACHE的属性能力，手机通过支持属性可以得知网关是新网关。Rf设备认证时flags 0x08表示新设备支持TT\_CACHE。Led灯特殊处理，TT报文都当做TT\_CACHE处理。

### IA.RFGW.LIST\_DIGEST

UCAT\_IA\_RFGW\_TT\_LIST\_DIGEST

网关向手机发送报文摘要，支持get，push操作，报文格式为：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 0 | | 1 | | 2 | 3 |
| seq | | | | | |
| 设备0 flag | 设备0变化次数 | | 设备0cache变化次数 | | Pad |
| 设备1flag | 设备1变化次数 | | 设备1cache变化次数 | | Pad |

网关向手机发送。

### IA.RFGW.LIST\_DIGEST\_ACK

UCAT\_IA\_RFGW\_TT\_LIST\_DIGEST\_ACK

手机向网关发送报文摘要ack，报文格式为：

|  |  |  |  |
| --- | --- | --- | --- |
| 0 | 1 | 2 | 3 |
| seq | | | |

手机向网关回应。

### IA.RFGW.LIST\_WITH\_ID

UCAT\_IA\_RFGW\_LIST\_WITH\_ID

网关当前在线设备列表，支持get操作，报文格式为：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | | | 3 |
| Dev-count | Totle-count | Reserved | | | |
| Dev1 ID | Reserved | Dev1 sn | | | |
| Dev1 sn | | | | | |
| Dev1 SubType | Dev1 ExType | | flags | TLV\_count | |
| TLV... | | | | | |
| .......(Next Dev) | | | | | |

flags:

bit0表示设备是否在线（1表示在线）

bit1 表示是否是新设备（1表示新设备）

bit2 表示设备正在绑定

bit3-bit7保留

手机get请求只填dev ID，其余填0。

TLV包含设备的一些属性，例如：

UCT\_VENDOR 设备vendor-id

UCT\_NAME 设备名称

UCT\_ETYPE 设备扩展类型（字符串）

UCT\_VERSION 设备版本

UCT\_PSK 设备共享秘钥（网关发给手机不包含pks，网关之间同步设备信息包含）

### IA.RFGW.TT

UCAT\_IA\_RFGW\_TT

手机和设备透传命令，支持get、set、push

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 0 | 1 | 2 | | 3 |
| Dev sn | | | | |
| Length | | | Data | |
| ..... | | | | |

### IA.RFGW.TT\_CACHE

UCAT\_IA\_RFGW\_TT\_CACHE

手机和设备透传命令，支持get、set、push

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 0 | 1 | 2 | | 3 |
| Dev sn | | | | |
| Length | | | Data | |
| ..... | | | | |

下面描述网关之间通过udp进行设备信息同步

网关之间通过ijconfig协议进行发现。发现漫游组内的网关后，约定sn小的主动发起连接。认证过程使用漫游组共享秘钥，网关之间认证过程同udp设备与服务器认证过程。网关之间建立连接后，进行保活并按需同步设备信息。

### IA.RFGW.DEV\_SYNC

UCAT\_IA\_RFGW\_DEV\_SYNC

网关之间同步设备信息，支持delete、get、push，报告格式参考UCAT\_IA\_RFGW\_LIST

### IA.RFGW.DEV\_GROUP

UCAT\_IA\_RFGW\_DEV\_GROUP

管理分组，支持set、get、delete

set创建或更新分组名称，Group-ID从1开始，DevCount填0

get查询分组，Group-ID为0时，查询所有分组，非0时，查询指定分组，网关返回分组信息包含分组成员

delete 删除分组，DevCount填0

|  |  |  |  |
| --- | --- | --- | --- |
| 0 | 1 | 2 | 3 |
| Group-ID | DevCount | Reserved | |
| GroupName  (16 bytes) | | | |
| SN1 | | | |
| SN2 | | | |
| ... | | | |

### IA.RFGW.DEV\_GROUP\_MEMBER

UCAT\_IA\_RFGW\_DEV\_GROUP\_MEMBER

管理分组成员，支持set、delete

set 添加分组成员，DevCount表示添加多少个SN

delete 删除分组成员，DevCount表示删除多少个SN

|  |  |  |  |
| --- | --- | --- | --- |
| 0 | 1 | 2 | 3 |
| Group-ID | DevCount | Reserved | |
| SN1 | | | |
| SN2 | | | |
| ... | | | |

### IA.RFGW.DEV\_GROUP\_TT

UCAT\_IA\_RFGW\_DEV\_GROUP\_TT

透传控制命令给分组设备，支持set、get

|  |  |  |  |
| --- | --- | --- | --- |
| 0 | 1 | 2 | 3 |
| Group-ID | Reserved | Length | |
| Data..... | | | |

### IA.RFGW.DEV\_NANE

UCAT\_IA\_RFGW\_DEV\_NAME

设置设备名称，支持set

|  |  |  |  |
| --- | --- | --- | --- |
| 0 | 1 | 2 | 3 |
| SN | | | |
| DevName  (16 bytes) | | | |

## UDP通信协议常量定义

//2.4G RF 网关

//设备子类型定义

#define IJ\_RFGW 0x1E

//采用6621模组的网关扩展类型定义

#define ETYPE\_IJ\_RFGW\_6621 0x01

//IA.RFGW

#define UCSOT\_IA\_RFGW 21

//IA.RFGW.JOIN

#define UCAT\_IA\_RFGW\_JOIN 1

//IA.RFGW.JOIN\_FIND

#define UCAT\_IA\_RFGW\_JOIN\_FIND 2

//IA.RFGW.JOIN\_ACTION

#define UCAT\_IA\_RFGW\_JOIN\_ACTION 3

//IA.RFGW.GROUP

#define UCAT\_IA\_RFGW\_GROUP 4

//IA.RFGW.LIST

#define UCAT\_IA\_RFGW\_LIST 5

//IA.RFGW.TT

#define UCAT\_IA\_RFGW\_TT 6

//IA.RFGW.DEV\_SYNC

#define UCAT\_IA\_RFGW\_DEV\_SYNC 7

//IA.RFGW.PARAM

#define UCAT\_IA\_RFGW\_PARAM 12

#define UCAT\_IA\_RFGW\_TT\_CACHE 13

#define UCAT\_IA\_RFGW\_LIST\_DIGEST 14

#define UCAT\_IA\_RFGW\_LIST\_DIGEST\_ACK 15

#define UCAT\_IA\_RFGW\_LIST\_WITH\_ID 16

## RF通信协议

这里的报文指2.4G帧格式中1～32字节的载荷部分。

由于RF载荷十分有限，而且具体产品的实际控制命令在透传数据里面，第一字节命令字段空闲位较多，现使用最高位作为加密标志，1表示后续载荷已经加密，0表示未加密。第一字节不加密。

### 申请配对

发送方向：设备→网关

接收地址：全网广播（P0）

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | 2 | 3 | 4 |
| cmd=申请配对 | 保留 | 设备主类型 | 设备子类型 |
| 设备序列号8字节 | | | |

保留字节的最低位作为旧设备标志，1表示曾经绑定过，0表示新设备。

### 允许配对

发送方向：网关→设备

接收地址：全网广播（P0）

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | 2 | 3 | 4 |
| cmd=允许配对 | 设备ID | 网关周期（2bit）+ 时间戳（14bit） | |
| 网关网络号4字节 | | | |
| 设备序列号8字节 | | | |

注：若网关不允许配对，则不发送报文

网关周期：0代表50ms，1代表100ms，2代表150ms，3代表200ms。

时间戳：网关周期内时间偏移量，单位为16us。

### 下发配对

发送方向：网关→设备

接收地址：单播（P1）

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | 2 | 3 | 4 |
| cmd=下发配对 | 保留 | | |
| 共享密钥8字节 | | | |

注：用户不确认，网关就不会下发最终配对报文，设备需要启动超时机制。

### 认证请求

发送方向：设备→网关

接收地址：单播-明文（P1）

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | 2 | 3 | 4 |
| cmd=认证请求 | 保留 | 设备主类型 | 设备子类型 |
| 设备序列号8字节 | | | |
| randem1 | | | |

### 认证提问

发送方向：网关→设备

接收地址：临时单播（P1）

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | 2 | 3 | 4 |
| cmd=认证提问 | 设备ID | 网关周期（2bit）+ 时间戳（14bit） | |
| 设备序列号8字节 | | | |
| randem2 | | | |

网关周期：0代表50ms，1代表100ms，2代表150ms，3代表200ms。

时间戳：网关周期内时间偏移量，单位为16us。

设备ID：0~127有效，其他数值代表注册失败。

### 认证答案

发送方向：设备→网关

接收地址：单播（P1）

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | 2 | 3 | 4 |
| cmd=认证答案 | 设备ID | support encrypt method | |
| 16字节答案  MD5(rand1 + rand2 + psk) | | | |

### 认证结果

发送方向：网关→设备

接收地址：单播（P1）

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | 2 | 3 | 4 |
| cmd=认证结果 | 认证结果 | selected encrypt method | |

如果认证通过并选择要加密，加密会话秘钥为MD5(rand1+rand2+psk+psk)

### 保活和命令下发

1. beacon若发送时间戳为0，则第一字节最高位置1，低7位0~127循环，表示周期序号。第二字节表示消息总数，设备列表中只包含省电设备。

beacon若发送时间戳不为0，则第一字节最高位置0，低7位填时间戳，第二字节0~127循环，表示周期序号。

beacon第三字节开始为有消息的设备列表，一个字节代表一个设备。

2. 0xF1及以上的地址保留做特殊用途。

3. ID为0~127的设备，在收到和ID相同的beacon序号，在第一个竞争周期发送keepalive给网关。

ID为128~256的设备，在收到和ID-128相同的beacon，在第二个竞争周期发送keepalive给网关。

设备发送keepalive最快的周期是25秒，但是设备可以间隔数个周期发送keepalive。

网关3个该接收keepalive的时间没有收到报文，就认为设备离线。

设备发送keepalive的时候，网关认为设备不在线，发报文告知设备离线，设备重新认证。

若设备长久没有收到网关的beacon报文，认为离线。

4. 省电设备可以以1,2,4,8个beacon周期接收beacon，接收beacon的时间要beacon序号整除自己的周期数。若某次接收beacon超时，则下个周期接着接收beacon，3次超时，发送对时报文到网关重新获取下一次beacon时间。

5. 设备认证时告知网关自己接收beacon的周期和keepalive的周期。网关在beacon的序号整除周期的时候发送第一个命令报文给设备，若没有ack，连续发送5个周期。网关回设备ack的时候，不用关心beacon序号而最快发送。

6.省电设备收到beacon中有自己的消息的时候，一直要收到没有自己的消息的beacon为止。

7. 网关向设备发送命令，连续2个命令都没有收到ack，认为设备离线。

8.当网关发现设备2个周期都没有回的时候，主动发送保活报文给设备询问是否在线，设备收到后回复，网关重试5次。

### Beacon

发送方向：网关→设备

接收地址：子网广播（P2）

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | 2 | 3 | 4 |
| 指示1bit + 时间戳7bit/周期序号 | 周期序号 | 设备ID1 | 设备ID2 |
| … … | | | |

注：设备在P2收到的报文，必为beacon报文。

beacon若发送时间戳为0，则第一字节最高位置1，低7位0~127循环，表示周期序号。第二字节表示消息总数，设备列表中只包含省电设备。

beacon若发送时间戳不为0，则第一字节最高位置0，低7位填时间戳，第二字节0~127循环，表示周期序号。

beacon第三字节开始为有消息的设备列表，一个字节代表一个设备。

时间戳：网关周期内时间偏移量，单位为16us。超过2ms，网关放弃本周期beacon发送。

设备IDn：有消息待发的设备列表，可以有0~10个。ID最高位为1，为强制设备发送保活报文。

### 保活报文

发送方向：设备→网关

接收地址：单播（P1）

|  |  |
| --- | --- |
| 1 | 2 |
| cmd=保活 | 设备ID |

### 网关向设备主动发送保活询问是否在线

发送方向：网关→设备

接收地址：单播（P1）

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | 2 | 3 | 4 |
| cmd=同步信息 | 序列号 | 子命令=保活 | 保留 |

### 网关向设备发送透传命令

发送方向：网关→设备

接收地址：单播（P1）

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | 2 | 3 | 4 |
| cmd=设备透传命令 | 序列号 |  |  |
| 透传命令分组… … | | | |

注：设备对命令处理快，可本周期应答手机APP，若处理不及时，尽量在本周期应答只带序列号的ACK。应答手机APP的透传分组使用推送的方式完成。

### 设备向网关发送透传应答

发送方向：设备→网关

接收地址：单播（P1）

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | 2 | 3 | 4 |
| cmd=设备透传应答 | 序列号 | 设备ID | 保留 |
| 透传应答分组… … | | | |

注：设备对命令处理快，可本周期应答手机APP，若处理不及时，尽量在本周期应答只带序列号的ACK。应答手机APP的透传分组使用推送的方式完成。

### 网关向设备发送透传命令获取通用缓存

发送方向：网关→设备

接收地址：单播（P1）

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | 2 | 3 | 4 |
| cmd=设备透传命令 | 序列号 | 透传命令分组 | |
| 透传命令分组… … | | | |

注：设备对命令处理快，可本周期应答手机APP，若处理不及时，尽量在本周期应答只带序列号的ACK。应答手机APP的透传分组使用推送的方式完成。

### 设备向网关发送透传应答发送通用缓存

发送方向：设备→网关

接收地址：单播（P1）

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | 2 | 3 | 4 |
| cmd=设备透传应答 | 序列号 | 设备ID | 保留 |
| 透传应答分组… … | | | |

注：设备对命令处理快，可本周期应答手机APP，若处理不及时，尽量在本周期应答只带序列号的ACK。应答手机APP的透传分组使用推送的方式完成。

### 推送透传请求,缓存

发送方向：设备→网关

接收地址：单播（P1）

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | 2 | 3 | 4 |
| cmd=推送透传请求 | 推送序列号 | 设备ID | 保留 |
| 推送消息内容分组 | | | |

注：设备推送给手机的信息，只需推送一次给网关，网关分发给多个手机。设备端不要每次推送所有信息。

### 推送透传应答，缓存

发送方向：网关→设备

接收地址：单播（P1）

|  |  |
| --- | --- |
| 1 | 2 |
| cmd＝推送透传应答 | 推送序列号 |

### 推送透传请求

发送方向：设备→网关

接收地址：单播（P1）

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | 2 | 3 | 4 |
| cmd=推送透传请求 | 推送序列号 | 设备ID | 保留 |
| 推送消息内容分组 | | | |

注：设备推送给手机的信息，只需推送一次给网关，网关分发给多个手机。设备端不要每次推送所有信息。

### 推送透传应答

发送方向：网关→设备

接收地址：单播（P1）

|  |  |
| --- | --- |
| 1 | 2 |
| cmd＝推送透传应答 | 推送序列号 |

### 网关向设备发送消息

发送方向：网关→设备

接收地址：单播（P1）

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | 2 | 3 | 4 |
| cmd=同步信息 | 序列号 | 子命令 | 保留 |
| 信息分组… … | | | |

### 设备向网关发送应答

发送方向：设备→网关

接收地址：单播（P1）

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | 2 | 3 | 4 |
| cmd=同步应答 | 序列号 | 设备ID | 保留 |
| 应答分组… … | | | |

### 推送请求

发送方向：设备→网关

接收地址：单播（P1）

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | 2 | 3 | 4 |
| cmd=推送请求 | 推送序列号 | 设备ID | 子命令 |
| 推送消息内容分组… … | | | |

### 推送应答

发送方向：网关→设备

接收地址：单播（P1）

|  |  |
| --- | --- |
| 1 | 2 |
| cmd＝推送应答 | 推送序列号 |

### 组播透传请求

发送方向：网关→设备

接收地址：组播地址

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | 2 | 3 | 4 |
| cmd=组播透传命令 | 序列号 | | |
| 分组设备位图（16 bytes） | | | |
| 透传命令分组 | | | |

为简化设备端代码适应低成本方案，设备端不参与分组管理。设备运行时，网关会给设备分配0到127的唯一ID，128位（16字节）设备分组位图的每一位对应一个设备ID，如果位图某一位是1，表示对应设备需要处理本透传控制命令。

网关发送组播控制命令后，还要逐个发送单播控制命令，一个目的是防止某些设备没有收到组播报文，另外是给设备分配回应单播ACK的时隙，避免设备回应ACK冲突。

安全考虑：

组播控制命令的安全性主要靠报文递增的序列号来抗重播。最快攻击按2毫秒一个报文计算，3字节（48位）的序列号在9.3小时翻转。另外组播序列号独立于单播序列号，网关启动时从0开始，设备连接到网关时，设备的组播序列号清零。

组播控制命令不加密，也很容易根据序列号递增规律构造攻击报文，因此需要加密。采用固定共享秘钥，tea算法进行加密。

### RF信号干扰解决

RF工作在2.4G频段，和wifi冲突。为了使得设备快速扫描到网关信道，我们只选择了4个信道2477M，2479M，2481M，2483M。这些频率都和wifi的13信道有冲突。当wifi使用13信道的时候，rf产生的电磁干扰使得wifi不能正常工作。为了避免这个情况，尽量使wifi和rf工作在不同的频率。

另在wifi的1信道选择2401M，2403M，2405M，2407M作为rf的选择频率。当wifi工作在7信道以上，rf就使用2401M~2407M中的频率，当wifi工作在7信道及以下，就选用2477M~2483M中的频率。

在一键配置没有成功的时候，不要让rf工作，避免一键配置不成功。

长久没连上wifi，网关的频率在wifi的1信道和wifi的13信道中切换。

网关较多时，自家的网关和邻居家的网关如果都使用一个信道，beacon发送时间可能慢慢地变到一起去，然后长久才分开。这样两个网关在长时间都在同一时间发送beacon，处于两个网关距离差不多的设备收到的信号就是错误的而收不到beacon。

为了避免这种情况，网关每隔5秒钟任选一个和其他报文不冲突的时刻发送一个信道占用指示报文。报文中包含序列号和周期内时间偏移量。网关若收到的序列号比自己的序列号小的信道占用指示报文，网关可以选择两种避让方式

1）若启动后信道切换次数小于3，则递增一个信道，并保存。递增的信道仍然遵循不和wifi冲突。

2）若启动后信道切换次数大于等于3，则不再切换信道。如果发现自己的beacon发送时间距离在区间[-3ms,3ms]之间，和则将自己的beacon发送时间都后推30ms。这样做的目的是在信道实在拥挤的情况下，错开时隙，保证beacon的发送时间是错开的，能正常被设备收到。而其他的命令报文发送不是很频繁并且有重发机制，也能收到。

### 信道占用指示报文

发送方向：网关→网关

接收地址：全网广播（P0）

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | 2 | 3 | 4 |
| cmd=信道指示 | 保留 | 时间偏移量 | |
| 设备序列号8字节 | | | |

### 升级协议

分配地址（配对）：

1）设备向网关发送gw\_config\_req\_t。

cmd=RF\_PACKET\_TYPE\_CONFIG\_REQ；

若激活信息有效，sn，dev\_type ext\_type从保存激活信息的flash中取。

若激活信息无效，sn=1，

flags = 2；用于和正常映像的配对请求区分开。

2）网关向设备回应gw\_config\_res\_t。

cmd=RF\_PACKET\_TYPE\_CONFIG\_RES

设备判断sn和发送的是否一致，若一致，根据client\_id和network\_id设置自己的接收地址。

----设备启动后，根据升级完成标志（校验）判断进入分配地址流程还是运行正常的映像。

升级：

1）网关向设备发送gw\_cmd\_t+rf\_upgrade\_req\_t，启动升级流程，告知映像头部。subcmd=RF\_SUBCMD\_UPGRADE。

---设备此时若运行的是正常映像，则清除升级完成标志。重启后先进入分配地址流程。网关会发送多次gw\_cmd\_t+rf\_upgrade\_req\_t，设备重启后还应收到。

2）设备端回应gw\_cmd\_ack\_t+rf\_upgrade\_res\_t，upgrade取值：0不升级，1要升级，2升级完成。subcmd=RF\_SUBCMD\_UPGRADE。

3）设备端向网关发送gw\_report\_t+offset\_list,subcmd=RF\_SUBCMD\_UPGRADE\_DATA

4)网关向设备发送gw\_upgrade\_t。

5）设备认为映像接收完成并检验成功后，向网关发送gw\_report\_t+rf\_upgrade\_res\_t，upgrade取值：0升级失败，2升级完成。subcmd=RF\_SUBCMD\_UPGRADE。升级若成功，设置升级完成标志。

## 网关设计

### 设备数据结构

#define CLIENT\_FLAGS\_VALID 0x01

#define CLIENT\_FLAGS\_DIRTY 0x02

#define CLIENT\_FLAGS\_ONLINE 0x04

#define CLIENT\_FLAGS\_AUTHED 0x08

#define CLIENT\_FLAGS\_CONFIGED 0x10

typedef struct {

UINT8 flags;

UINT8 seq\_send; //跟踪发送序列号

UINT8 seq\_recv; //跟踪推送序列号

UINT8 pad;

UINT32 alive; //keepalive 收到的时间

UINT8 sn[8]; //设备sn

char psk[8]; //分配的设备共享密码

UINT32 rand1; //随机数1

UINT32 rand2; //随机数2

} SSV7241\_client\_t;

SSV7241\_client\_t SSV7241\_client[128] = {0};

注：psk及以后的字段，认证完成后，用作保存加密信息。

### 发送队列

队列元素：

typedef struct {

struct stlc\_list\_head link;

UINT8 client\_id;

UINT8 len;

UINT8 seq;

UINT8 retry;

Char buf[32];

} SSV7241\_queue\_node\_t;

数据来源：网关向设备发送消息，回应设备推送消息的ACK。

client\_id+seq可唯一标识一消息，重发的消息seq不变。

发送队列采用链表保存，网关每个周期原则上取队列头的16个消息发送，但会处罚retry次数过多的报文。

如果是命令消息，发送后不删除，收到ack或超次或设备离线后才删除。

如果是ACK类，发送后立即删除。

对外提供入队函数。

### 接收队列

队列元素和发送队列相同。

数据来源：设备向网关推送消息，设备回应网关的ACK（带数据）。

client\_id+seq可唯一标识一消息，重发的消息seq不变。

收到ACK报文将对应的发送队列元素删除，不放入接收队列中。

新seq报文放到本地套接字中，利于zebra框架接收。

本地消息处理后，立即删除。

发送给手机的报文，需要收到ACK后，才删除。