**讯群腕表TCP通信文档**

0x01 登录 5

0x02 身份信息变化通知 6

0x03 获取当前时间戳 6

0x04 设置心跳间隔 6

0x05 上传定位 7

0x06 联系人列表变化通知 8

0x07 脱落报警 8

0x08 激活腕表 8

0x0a 解绑腕表 8

0x0b上传静音状态 8

0x0c家庭圈新消息 9

0x0e 请求持续定位 9

0x10 结束持续定位 9

0x12 锁定腕表 9

0x14 解锁腕表 10

0x16 监听腕表 10

0x17 上传电量百分比 10

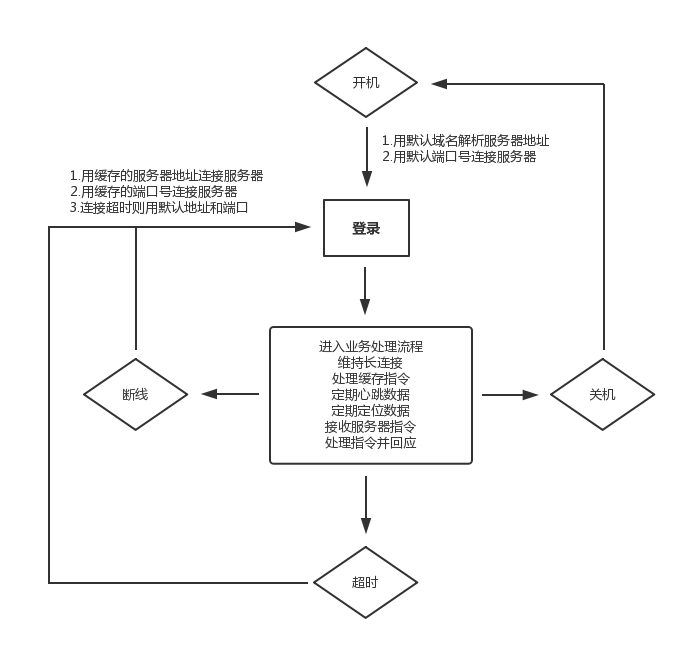
0x18 重新登陆 10

0x1a 重启腕表 10

0x1b 腕表低电量即将休眠 10

0x1c 开启飞行模式 10

1. 腕表与服务器TCP通信流程



1. 腕表开机时用默认域名，默认端口登陆服务器，为TCP长连接方式；

2. 默认每隔5分钟发送腕表心跳包（上传定位数据），维持长连接在线，不启用TCP Keep-alive参数，使用心跳包维持连接；

3. 所有指令的默认超时时间为15s；

4. 作为心跳包上传定位信息时，每次开机时为上次0x04指令设置的心跳间隔，如果没有设置过心跳间隔，则默认为5分钟；

5. 腕表发送任何指令在超时时间内未收到服务器确认包，则连接超时，将自身心跳间隔减少1分钟，心跳间隔最少1分钟，重新登陆后发送未发送成功的指令；

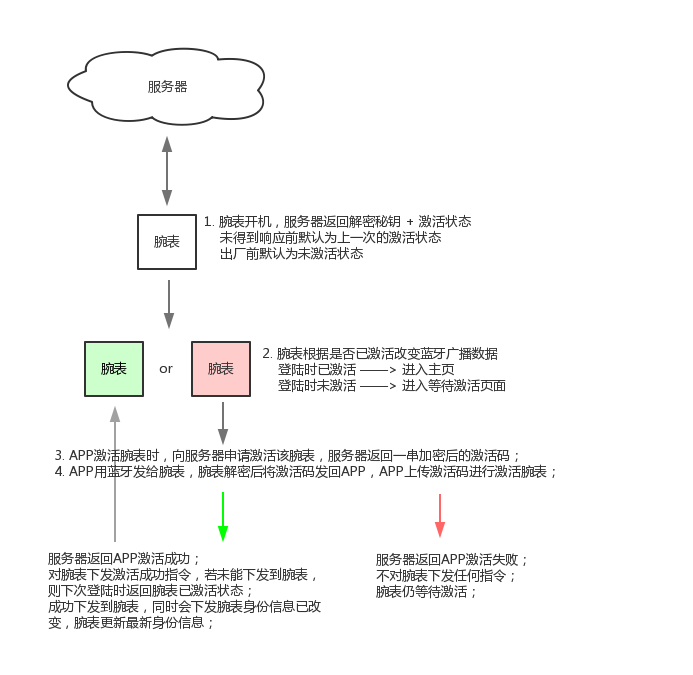
6. 如果登陆时服务器返回确认中带有重定向参数 (新服务器地址、端口)，则腕表使用新的服务器地址和端口进行登录，直到返回登陆成功；

协议中默认的服务器地址为：[s.xunqun.net:8000](http://watch.xunqun.net:8000)

协议示例imei为：355372020827303；

**激活：**

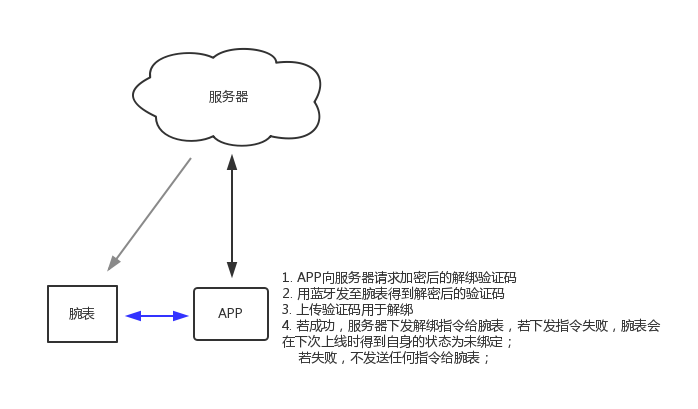
默认腕表为未激活状态，需要由APP激活后使用，激活流程：



**解绑：**

腕表在收到服务器解绑指令，或登录指令返回值收到的腕表状态位为未绑定时，将自身状态视为未绑定，将之前的信息删除，恢复到出厂设置。

静音设置为关，名字为空(或默认?)，头像为默认图片，联系人列表为空，等待APP激活，此时仍上传定位（心跳包），以保证服务器能及时下发激活指令，以及身份信息修改通知。



1. 通信指令格式

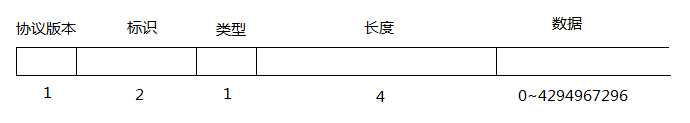
1. 腕表与服务器的通信指令中目前只含有控制指令，不含有语音图片等数据流（语音、图片用http接口进行上传下载）；

2. 指令用大端方式传输；

3. 腕表主动上传的指令指令类型为奇数；

4. 服务器主动下发的指令指令类型为偶数；

5. 指令中的字符串编码使用utf-16（大端、不带BOM）；



6. 协议头部为1字节版本字段，当前协议版本号为 0x00；

7. 标识字段用于标识腕表和服务器之间每次指令，由主动发起指令的一方生成，返回一方返回确认时标识字段与收到的指令对应相同，2字节；

8. 类型字段为1字节；

9. 长度字节为4字节，标识指令所带数据长度；

10. 数据字段，可选部分，数据的格式各个不同指令不同；

1. 各指令类型数据格式

各指令示例中

1. 包含 ' ' 的为utf-16BE字符串；

2. 包含 \x 开头为16进制；

3. 其他为数字类型；

各指令中填充字段仅用于4字节对齐；

## 0x01 登录

1. 腕表端发送数据：

|  |  |  |
| --- | --- | --- |
| 字段 | 长度 | 示例 |
| imei | 8 byte | 355372020827303 |
| imsi | 8 byte | 460001515535328 |
| 蓝牙mac地址 | 8 byte | \x00\x00\xc4\x54\x44\x58\xcb\x7a |
| 心跳间隔 | 4 byte | 300 |
|  |  |  |

imei、imsi为腕表自身属性，数字类型；

蓝牙地址前两个为对齐的\x00，后面为mac地址字节表示；

imei = 355372020827303

imsi = 460001515535328

mac = c4544458cb7a

eg:

0x00abcd0100000028\_000143357f1084a7\_0001a25e72edfbe0\_0000c4544458cb7a\_0000012c

2. 服务端返回：

(1). 登陆成功时返回：

|  |  |  |
| --- | --- | --- |
| 字段 | 长度 | 示例 |
| 登陆状态 | 1 byte | 1 |
| 腕表状态 | 1 byte | 1 |
| 解密秘钥 | 10 bytes | 'abcde' |

腕表状态有：

1：已激活未锁定

2：已激活已锁定

3：未激活

解密秘钥：

可以用来鉴权APP发送过来的关于对腕表的操作是否有权限，APP从服务器获取密文，经腕表解密后，得到原始验证码，之后上传给服务器进行相关操作；

可以用来鉴权腕表通过http发送语音时的腕表身份，用于session参数；

腕表服务器之间的加密算法：

使用AES-192算法加密，mode为ECB，算法key为 imei+解密密匙+'1234'（共24位长），原文不足16位倍数的用空格补齐，腕表端解密之后将解密后的原文尾部空格删除；

eg：

key = '355372020827303abcde1234'

原文 = 'NeedAuthorization'

原文补足 = 'NeedAuthorization '

密文 = 0x4eee320adad4a543d701bfa20d3add18c4af7d961563535fc9bee0cd9975218a

eg:

0x00abcd010000000a\_01\_01\_00610062006300640065

(2). 登陆需要重定向时返回：

|  |  |  |
| --- | --- | --- |
| 字段 | 长度 | 示例 |
| 登陆状态 | 1 byte | 2 |
| 填充字段 | 1 byte | 0 |
| ip[0] | 1 byte | 172 |
| ip[1] | 1 byte | 16 |
| ip[2] | 1 byte | 1 |
| ip[3] | 1 byte | 1 |
| port | 2 byte | 123 |
| 填充字段 | 4 byte | 0 |

需要重定向：

ip、port为需要重定向过去的服务器地址，得到重定向回复后，腕表用得到的服务器地址和端口号进行登录；

之前是腕表状态字节的字段为填充字段，因为腕表重新登陆最后会获得腕表的当前状态，重新登陆期间的状态保持为上次开机的状态；

填充字段仅用于对齐；

eg:

0x00abcd010000000a\_02\_00\_ac100101007b00000000

## 0x02 身份信息变化通知

1. 服务端发送

0x00459a0200000000

2. 腕表端返回

0x00459a0200000000

腕表通过：

<http://www.xunqun.com:8001/watch/info?session=abcde&imei=355372020827303>

http接口所用的session为腕表登陆成功后服务器返回的解密秘钥字段；

获取到宝贝身份信息，接口见讯群腕表http通信文档；

## 0x03 获取当前时间戳

1. 腕表端发送：

0x00674a0300000000

1. 服务端返回：

|  |  |  |
| --- | --- | --- |
| 字段 | 长度 | 示例 |
| 时间戳 | 4 byte | 1439728484 |

时间戳为UTC时间戳；

eg:

0x00674a0300000004\_55d08364

## 0x04 设置心跳间隔

1. 服务端发送：

|  |  |  |
| --- | --- | --- |
| 字段 | 长度 | 示例 |
| 心跳间隔秒数 | 4 byte | 120 |

腕表未设置时，以及未遇到过指令超时的情况时，默认心跳间隔为300秒；

0x00a7fe0400000004\_00000080

1. 腕表端返回：

0x00a7fe0400000000

## 0x05 上传定位

1. 腕表端发送：

|  |  |  |
| --- | --- | --- |
| 字段 | 长度 | 示例 |
| type 定位类型 | 1 byte | 1 |
| lon 经度整数位 | 1 byte | 114 |
| lon 经度小数位 | 4 byte | 356170 |
| lat 纬度整数位 | 1 byte | 34 |
| lat 纬度小数位 | 4 byte | 824230 |
| mcount 基站数目 | 1 byte | 2 |
| mcc 国家编号 | 2 byte | 460 |
| mnc 运营商编号 | 2 byte | 0 |
| lacid 小区编号 | 2 byte | 9475 |
| cellid 基站编号 | 2 byte | 44901 |
| level 信号强度 | 4 byte | -78 |
| timestamp 时间戳 | 4 byte | 1432568387 |

定位类型：

1：定期定位（心跳）

2：服务器下发持续定位之后返回的定位

经纬度：

没有GPS的经纬度信息时，lat和lon整数与小数位数值为 0；

lat、lon整数位最大180，小数位最大999999；

如133.003456：分解为整数位133，小数位3456；

信号强度字段为原始数值减去110的数值，即 dB；

mcount字段即采集的基站信息数目最多6组；

type = 1

lat = 114.356170

lon = 34.824230

mcount = 2

mcc = 460,460

mnc = 0,0

lacid = 9475,9475

cellid = 44901, 44901

level = -78,-78

timestamp = 1432568387

eg:

0x0095c0050000001c\_01\_72\_00056f4a\_22\_000c93a6\_02\_01cc\_0000\_2503\_af65\_ffffffb2\_01cc0000\_2503\_af65\_ffffffb2\_55634243

2. 服务端返回：

0x0095c00500000000

## 0x06 联系人列表变化通知

1. 服务端发送

0x0065230600000000

2. 腕表端返回

0x0065230600000000

腕表通过：

<http://www.xunqun.com:8001/watch/contractbook?session=abcde&imei=355372020827303>

获取到宝贝联系人列表，接口见讯群腕表http通信文档；

## 0x07 脱落报警

1. 腕表端发送：

|  |  |  |
| --- | --- | --- |
| 字段 | 长度 | 示例 |
| 时间戳 | 4 byte | 1439728484 |

时间戳为发生该动作的时间戳

eg：

0x0076ac0700000004\_55d08364

1. 服务端返回：

0x0076ac0700000000

## 0x08 激活腕表

1. 服务端发送：

0x00e73a0800000000

1. 腕表端返回：

0x00e73a0800000000

## 0x0a 解绑腕表

1. 服务端发送：

0x0065210a00000000

1. 腕表端返回：

0x0065210a00000000

## 0x0b上传静音状态

1. 腕表端发送：

|  |  |  |
| --- | --- | --- |
| 字段 | 长度 | 示例 |
| 当前静音状态 | 4 byte | 1 |

静音状态：

0：腕表静音状态为关

1：腕表静音状态为开

eg:

0x0065210b00000004\_00000001

1. 服务端返回：

0x0065210b00000000

## 0x0c家庭圈新消息

1. 服务端发送：

|  |  |  |
| --- | --- | --- |
| 字段 | 长度 | 示例 |
| 消息类型 | 4 byte | 1 |
| session | 4 byte | 1439728484 |
| 消息id | 48 byte | '55f43cb60bdb82a0fd9ff49c' |

消息类型：

1：消息为语音类型

2：消息为图片类型

3：消息为文本类型

eg:

0x0076560c00000038\_00000001\_55d08364\_003500350066003400330063006200360030006200640062003800320061003000660064003900660066003400390063

1. 腕表端返回：

0x0076560c00000000

腕表通过：

<http://www.xunqun.com:8001/watch/message?session=abcde&imei=355372020827303&id=55f43cb60bdb82a0fd9ff49c&type=1>

获取到家庭圈该条消息，接口见讯群腕表http通信文档；

## 0x0e 请求持续定位

1. 服务端发送：

|  |  |  |
| --- | --- | --- |
| 字段 | 长度 | 示例 |
| 定位次数 | 2 byte | 5 |
| 每次定位间隔秒数 | 2 byte | 1 |

当定位次数为1（定位间隔秒数被忽略）时，效果为立即请求一次定位；

0x0084210e00000004\_00050001

1. 腕表端返回：

0x0084210e00000000

## 0x10 结束持续定位

1. 服务端发送：

结束腕表上一次收到的持续定位，若当前没有正在进行的持续定位，则忽略这次指令；

0x0056540f00000000

1. 腕表端返回：

0x0056540f00000000

## 0x12 锁定腕表

1. 服务端发送：

0x00e34a1200000000

1. 腕表端返回：

0x00e34a1200000000

## 0x14 解锁腕表

1. 服务端发送：

0x00776a1400000000

1. 腕表端返回：

0x006a1400000000

## 0x16 监听腕表

1. 服务端发送：

0x003a441600000000

1. 腕表端返回：

0x003a441600000000

## 0x17 上传电量百分比

1. 腕表端发送：

|  |  |  |
| --- | --- | --- |
| 字段 | 长度 | 示例 |
| 电量百分比 | 4 byte | 5 |

0x0055511700000004\_00000005

2. 服务端返回：

0x0055511700000000

## 0x18 重新登陆

1. 服务端发送：

0x00854a1800000000

2. 腕表端返回：

0x00854a1800000000

## 0x1a 重启腕表

1. 服务端发送：

0x0078121a00000000

2. 腕表端返回：

0x0078121a00000000

## 0x1b 腕表低电量即将休眠

1. 腕表端发送：

0x0087631b00000000

2. 服务端返回：

0x0087631b00000000

## 0x1c 开启飞行模式

1. 服务端发送：

0x0045621c00000000

2. 腕表端返回：

0x0045621c00000000