# 系统通信协议设计V5.3

易发胜 2017-5-27

[〇、名词解释](#_Toc4561)

[一、报文基本格式](#_Toc12715)

[1、基本首部](#_Toc30248)

[二、具体协议格式说明](#_Toc8383)

[0、登录帐号的形成](#_Toc19520)

[1、连接管理协议](#_Toc19868)

[2、平台帐号管理协议](#_Toc27868)

[3、控制协议](#_Toc22611)

[4、数据查询协议](#_Toc24760)

[5、消息传递协议](#_Toc13271)

[6、局域网发现协议](#_Toc20353)

[7、文件信息传输协议](#_Toc28576)

[8、加密通信协议](#_Toc24416)

[9、关联管理协议](#_Toc25465)

[10、联系人管理协议](#_Toc21011)

[11、升级查询协议](#_Toc30402)

## 〇、名词解释

前端设备：被管理和控制的设备，包括前端监控设备和监控APP

管理APP：可对前端设备进行管理的android APP程序

管理员：对web服务器平台进行管理的人员

用户：使用管理APP登录平台的各类人员

联系人：用户使用管理APP添加的其他平台用户帐号

关联人：使用管理APP对前端设备进行操控或者接收其信息的用户

管理关联人：对前端设备具有管理权限的关联人

用户帐号：用户使用的、用来登录设备和平台的字符串，需要确保唯一性。

设备帐号：前端设备登录平台的帐号，可以使用IMEI或者MAC地址或者其他内置唯一标识符表示。

ID：由系统在用户或者设备注册时产生的，用来唯一标识系统一个用户的编号，由4个字节的整数构成。

平台：Web服务器或者由多个服务器构成的集群系统。

## 一、报文基本格式

所有报文采用二进制和JSON格式混合的格式，由基本首部、扩展首部及数据选项构成。其中，基本首部是所有子协议都必须包含的、必要的信息。

所有程序和设备通信通过UDP实现，皆绑定固定端口5678。

基本的数据格式如下：

ZNAF基本首部{ HOPT:{首部选项},DATA:{数据选项}}

基本首部包含如下数据域，其含义如表1-1。

表1-1 智能监控系统通信协议首部选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 数据域 | 类型 | 描述 |
| 基本首部 |  |  |  |
| 1 | CMD | 字节型1 | 协议类型 |
| 2 | TYPE | 字节型1 | 报文类型 |
| 3 | OPT | 字节型1 | 标记域，包括是否转发位 |
| 4 | SORT | 字节型1 | 发送者类型 |
| 5 | SID | 整数4 | 发送者报文的设备ID |
| 6 | SEQ | 整数4 | 发送序号 |
| 7 | ACK | 整数4 | 确认序号 |

### 1、基本首部

共五个域，以ZNAF开始，字母F后的数据采用二进制表示，共16个字节。下面分别说明：

CMD为子协议类型域。含义如下：

0：连通测试报文；

1：连接管理协议；

2：平台帐号管理协议；

**3：控制协议；**

4：数据查询协议；

5：消息传递协议；

**6：局域网发现协议；**

7：文件信息传输协议；

**8：加密协议；**

9：关联人管理；

10：联系人管理；

11：升级查询；

其中，连通测试报文仅仅用来测试目的程序是否工作，只需要基本首部，不需要任何扩展首部和数据选项。发送方发送CMD=0，TYPE=1的报文，接收方立即回答同样类型CMD=0,TYPE=2的报文即可。由于简单，在下面不再详细说明。注：回答报文要求序号符合如下直接首部的统一规定。

OPT 选项：按位有效，说明是否转发、是否加密、是否需要确认（请求报文）、是否确认报文等。

第0位，即1时，**表示此报文在服务器进行转发处理；**

第1位，即2时，**表示此报文加密处理过；**

第2位，即4时，**表示此报文携带源地址，便于NAT穿透处理**

第3位，即8时，表示此报文是请求报文或者需要确认的报文；

第4位，即16时，表示此报文是应答报文，确认号有效；

第5位，即32时，表示此报文后面有非JSON格式数据，主要用于传输有二进制格式数据，不能完全使用JSON解析器进行解析。详见文件信息传输协议说明。

注：OPT选项可以叠加。比如双向数据传输时，往往传给对方的报文中也含有对对方的确认（16），传输的数据可能加密了（2），是前端设备和管理APP之间通过服务器中转传输的（1），这样所有对应位都该置1，则OPT=1+2+16=19。

OPT的选项决定了HOPT首部是否存在，具体逻辑如下：

如果OPT第0位置1，扩展首部HOPT中需要有DID选项，说明转发目的地；

如果OPT第1位为1，表示DATA内容加密过，需要扩展首部HOPT有密钥序号KEYSEQ选项。

如果OPT第2位置1，表示携带有发送方的源IP和端口，HOPT有SIP和SPORT选项。

SEQ，ACK发送和确认序号：**每个发送的报文都有唯一的发送序号**；需要应答时，需要ACK序号，ACK的值是收到请求报文的序号，具有相关性。

SID表示发送报文的用户或者设备的ID，为一个4字节整数，表示设备或者用户在平台上的唯一编号。没有在平台注册时，ID恒定为0。ID<10000时，表示服务器ID范围。

SORT表示发送方的类别。**0代表使用管理app的用户类，1代表APP监控虚拟设备类，2代表LINUX监控前端设备类，3代表web服务器类**。注意：经服务器中转报文的类别保持不变。

TYPE表示某个协议的报文类别，含义如下面具体协议所述。

连通测试协议仅仅只有基本首部，但是要求CMD=0，TYPE=1或者2，OPT=8或者16；表示要求确认或者应答报文。用户没有登录时也可以用此协议，这时没有SID, SID值为0。

下面详细说明其他各协议的具体要求。

## 二、具体协议格式说明

### 0、登录帐号的形成

登录帐号一般使用设备所用的唯一标识符，如IMEI或者电话号码。最长允许不超过20个字符。其中用户注册信息要求电话号码，便于用户不在线时，可以扩展支持发送短信。也方便对短信验证码的验证支持。管理员帐号可使用邮箱或者其他自然名称。设备帐号可采用设备中存在的唯一标识符，如mac地址、IMEI、电话号码或者其他标识符。

每个帐号在登录之前先要注册，注册时会检查帐号的唯一性。

系统的任何类型帐号使用平台之前，应该先登录平台。平台服务器地址端口应该在是各个可登录程序的一个配置。

### 1、连接管理协议

连接管理协议用于管理APP用户登录平台和监控设备（移动监控APP或者前端设备）、以及前端设备登录平台等场合。

连接管理采用四次握手的登录协议。但是被登录方可以配置只要两步就同意登录。

CMD=1表示连接管理协议。

1、登录请求

2、登录应答

3、验证请求

4、验证应答

登录方（管理APP，前端设备）

被登录方（平台，前端设备）

#### 1.1 登录请求

考虑系统中软件有第三方开发，可能还有版本改进。因此，登录请求需要传输软件信息。TYPE=1，具有选项如表2-1。

表2-1 登录请求报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | SNUM | 字符串 | 软件编号，8个数字。 |
| 2 | SVER | 字符串 | 软件版本号，6个十六进制数xxyyzz |
| 3 | USER | 字符串 | 用户帐号：8-20个字符构成字符串 |
| 4 | LINK | 整数 | 短暂离线后快速登录时使用（可选） |

监控APP或者前端设备等待用户登录时，不能接受SORT=0以外的报文登录。也就是说，它们只接收管理APP用户类型登录。

SNUM、SVER、SORT是程序内置的固定值，需要有配置项让用户配置USER。并且在服务器上检查USER的唯一性。详见下面的帐号管理协议。

注：如果管理APP未注册也未登录平台，直接在局域网内登录监控APP或者前端设备，则不一定能够保证USER的唯一性。由被登录设备在关联时确保所有可登录其上的用户帐号唯一即可。没有在平台注册时，在局域网登录前端设备，基本首部的SID为0，让前端设备知道管理APP用的是临时账号。

如果用户因为短暂断网要求快速登录，可以使用以前获得的LINK实现快速登录，而不需要再验证密码。

#### 1.2 登录应答

被登录方收到登录请求报文后，检查相应的信息，并根据配置确定是否需要密码验证。TYPE=2，其他选项如表2-2。

表2-2 登录应答报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | RET | 字符串 | 返回代码，0表示通过登录验证；-1表示出错；1表示需要验证。 |
| 2 | LINK | 整数 | RET=0时有效，增强安全性（可选） |
| 3 | INFO | 字符串 | 错误原因、随机数或登录者ID，  当RET=-1时错误原因；  当RET=1时为随机数字符串；  当RET=0时返回登录者的ID。如果登录前端设备，前端设备将SID作为登录ID返回。登录分配的LINK需要保存起来，以备后用。 |

各个被登录方在前期为了简化开发，收到用户名可以直接返回登录成功，不需要密码验证。注意：有时候，登录方可能短暂断网，重新登录，如果被登录方发现登录方以前的状态信息，可以根据策略不需要登录方继续验证（即使配置了需要验证），这时候可以修改其被登录的状态信息，直接通知登录成功。错误原因用“代码:字符串”方式表示，计算机通过检查代码可以知道错误具体原因，人通常看字符串。

如果发送登录报文后没有收到应答，则每30秒钟（可配置）重新发送一次登录报文。

#### 1.3 验证请求

被登录方要求登录方提供验证时，登录方提供验证信息。TYPE=3，其他选项如表2-3。

表2-3 验证请求报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | CODE | 字符串 | 先对随机数用密码加密，采用XOR加密。然后对加密的数据用base64编码。 |
| 2 | USER | 字符串 | 用户帐号：8-20个字符构成字符串 |

#### 1.4 验证应答

被登录方收到登录请求报文后，检查相应的信息，并根据配置确定是否需要密码验证。TYPE=4，其他选项如表2-4。

表2-4 验证应答报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | RET | 整数 | 返回代码，0表示通过登录验证；-1表示出错。 |
| 2 | LINK | 整数 | RET=0时有效，可增强安全性（可选） |
| 3 | INFO | 字符串 | 错误原因、登录者ID，当RET=-1时错误原因；当RET=0时返回登录者ID。如果登录前端设备，前端设备并不检查SID正确性，直接返回验证请求报文的SID即可。 |

#### 1.5 登出请求

任何一方可以主动发出登出报文，登出报文不需要确认信息，是一个单方面报文。TYPE=5，其他选项如表2-5。

表2-5 登出请求报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | USER | 字符串 | 用户帐号：8-20个字符构成字符串 |
| 2 | LINK | 整数 | 增强安全性（可选） |

登出时，被请求方需要认证核对相关信息如SID等，防止攻击误删状态信息。

#### 1.6 保活报文

登录后，如果30秒内双方没有通信信息，要求登录方主动发送保活报文。维持通信关系。登录方主动发送，被登录方及时应答。TYPE=6，没有选项。

如果保活3次没有成功，则进入重新登录状态。

如果一个管理APP通过中转登录了监控APP或者监控设备，保活报文也需要中转。一个中转保活报文可以同时对平台和前端设备进行保活。

#### 1.7 保活应答报文

被登录方收到保活报文后，立即向登录方回复保活应答报文。接收方可通过确认号对比原来的发送号来判断是否前面的保活请求。TYPE=7，没有选项。

### 2、平台帐号管理协议

平台帐号管理协议是前端设备和管理APP申请或者注册平台的登录帐号用的，包含2个处理过程：注册帐号和删除帐号。（变更帐号功能待今后扩展）

CMD=2表示平台帐号管理协议。

1、注册帐号请求

2、注册帐号应答

3、修改帐号请求

4、修改帐号应答

5、注销帐号请求

6、注销帐号应答

平台

登录方（前端设备和管理APP）

#### 2.1 注册帐号请求

每个接入平台服务器的设备或者软件都有一个独一无二的帐号。该帐号是唯一的、用于不同用户之间进行识别和管理。TYPE=1，其他选项如表2-6。

帐号的形成操作不需要登录服务器，可以根据用户意愿形成，只要确保唯一即可。今后可能需要在界面检验是否有重复。

表2-6 申请帐号报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | SNUM | 字符串 | 软件编号，8个数字。 |
| 2 | SVER | 字符串 | 软件版本号，6个十六进制数 |
| 3 | USER | 字符串 | 用户帐号：8-20个字符构成字符串 |
| 4 | PASSWORD | 字符串 | 密码 |
| 5 | INFO | 字符串 | 注册辅助信息，不同类型要求不同。由JSON格式表示。 |

如上表所示，所有字段与登录申请类似，但是web服务器并不记录状态，检查这些软件和用户名是否符合要求、是否有重复后应答。INFO是注册辅助信息，对于APP包括自动权限，名字，出生年月，性别，邮箱，类型，手机号等7个内容。其JSON名字为：LIMIT，NAME，BIRTH，SEX，EMAIL，CLASS，PHONE”这样的格式构成。对于前端设备，包括序列号，条形码，经度，维度，最大关联人数量，类型，手机号等信息，构成格式类似前面所述，JSON关键字为：SEQ，BARCODE，LONGI，LATI，MAX，CLASS，PHONE。如果只是想获得以前注册的用户ID，则不需要INFO选项。

#### 2.2 注册帐号应答

Web服务器收到帐号申请报文后，检查软件是否许可，账号是否重复，登记新帐号到数据库中。TYPE=2，其他选项如表2-7。

表2-7 申请帐号报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | RET | 整数 | 返回代码，0表示通过申请验证；-1表示帐号申请失败；1表示帐号存在。 |
| 2 | INFO | 字符串 | 错误原因或者ID，当RET=-1时错误原因；当RET>=0时为帐号成功申请后的ID。 |

注：有时候，如果服务器返回应答失败，也许是申请方重复申请造成的。web服务器需要能够辨别是否恶意重复申请。比如记录申请者的当前网络地址信息和时间对比信息，避免注册攻击。

申请成功的帐号如果一定时间内（可服务器设置）没有使用，系统自动删除，需要重新申请才可用。因此也不需要删除帐号的有关协议报文。

用户在新的手机上登录时，可能因为没有保存以前申请的编号ID而重新注册，只有当重新申请的帐号密码都和系统保存的一致时，返回RET=1并返回ID。

#### 2.3 修改帐号请求

修改帐号是对帐号的资料进行修改，必须在登陆状态下进行。TYPE=3，其他选项如表2-8。

表2-8修改帐号请求报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | USER | 字符串 | 用户帐号：8-20个字符构成字符串 |
| 2 | LINK | 整数 | 增强安全性（可选） |
| 3 | PASSWORD | 字符串 | 修改后的用户密码（如果没有密码修改，不出现此选项） |
| 4 | INFO | 字符串 | 依次填写新的辅助信息。（如果没有一个辅助信息修改，协议可以不出现此选项） |

如上表所示，与帐号注册类似，唯一不同的是，user需要先登录并在基本首部域有sid信息才行。web服务器验证帐号，如果帐号不存在或者相关资料不匹配，都将不成功。

注意：此请求必须在登陆状态下进行。

#### 2.4 修改帐号应答

Web服务器收到帐号修改报文后，检查相应的信息，执行修改要求。

TYPE=4，其他选项如表2-9。

表2-9 修改帐号报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | RET | 整数 | 返回代码，0表示通过变更；-1表示帐号变更失败；1表示帐号已经这样变更过。 |
| 2 | INFO | 字符串 | 错误原因、时间，当RET=-1时错误原因；当RET>=0时为帐号变更成功后用户的ID（大多没有变化） |

#### 2.5 注销帐号请求

注销帐号需要在帐号登录后进行。TYPE=5，其他选项如表2-10。

表2-10 注销帐号请求报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | USER | 字符串 | 要注销的帐号，8-20个字符 |
| 2 | LINK | 整数 | RET=0时，可传输连接号增强安全性（可选） |
| 3 | INFO | 字符串 | 用户密码加密的电话号码base64编码 |

需要检查USER的INFO信息是否匹配原来登记的。

#### 2.6 注销帐号应答

Web服务器收到注销帐号请求报文后，检查相应帐号是否存在，提供信息是否正确，然后更正数据库，对此帐号所有相关关联人和联系人发出通知，然后才给出确认报文。TYPE=6，其他选项如表2-11。

表2-11 注销帐号应答报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | RET | 整数 | 返回代码，0表示通过注销；-1验证失败；1表示帐号已经注销过。 |
| 2 | INFO | 字符串 | 错误原因或者注销时间，当RET=-1时为错误原因；>=0时为注销帐号成功的时间 |

### 3、控制协议

控制协议是管理APP上的关联人对前端设备的控制操作，主要包括控制和查看两类操作（对前端设备的关联人管理具有另外的协议。

1、控制请求

2、控制应答

管理APP

前端设备

web中转

#### 3.1 控制请求

控制请求是管理端向监控端发送的控制命令，包括远程设置、远程控制和远程查询等命令，监控端需要检查用户是否登录认证，并检查是否具有相应的权限。

CMD=3表示控制协议；TYPE=1时，其他选项如表2-12。

表2-12 控制请求报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | USER | 字符串 | 请求者帐号，8-20个字符 |
| 2 | INST | 字节型 | 指令代码：0获取最近报警信息；1获取当前登录账户；2强制登录账号离线；3获取配置信息；4获取日志信息；5获取当前图片；6获取当前实时视频；7 获取插件信息；10自定义命令 |
| 3 | PARA | 字符串 | 命令参数：0-1限制数量；2账号；5分辨率；6实时视频参数；10具体自定义命令所需参数，没有就填0 |
| 4 | LINK | 整数 | 增强安全性（可选） |

INST和PARA可扩展。协议需要定义更加详细，对每种控制要求，核实具体的命令要求和返回信息格式。

#### 3.2 控制应答

监控端收到控制请求后，验证信息，执行控制操作，然后返回结果。TYPE=2，其他选项如表2-13。

表2-13 控制应答报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 2 | RET | 整数 | 返回代码，-1表示请求失败；0-n表示控制成功。  不同代码表示成功后返回信息类别  0：文本信息  1：文件信息  2：Base64编码的二进制信息  3：自定义信息，与请求的自定义命令有关 |
| 3 | INFO | 字符串 | 错误原因，格式：错误代码:错误信息  或控制结果信息，具体如下：  文件信息：文件名  二进制信息：base64编码  自定义信息：自定义 |

### 4、数据查询协议

#### 4.1 数据查询请求

数据查询请求是可用来查询web或者前端设备的一些信息，比如对方的id，各类未读消息等。一般在刚登录成功后使用，便于及时获取离线期间的未读信息。

CMD=4表示数据查询协议；TYPE=1时表示查询请求，其他选项如表2-14。

表2-14 数据查询请求报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | USER | 字符串 | 请求者帐号，8-20个字符 |
| 2 | CODE | 字节型 | 数据查询代码，具体如下，可以扩展：64用户id；0所有未读信息数量数；1未读报警消息数；2未读聊天消息数；4未读系统通知数；8未读联系人通知数；16未读关联通知数。 |
| 3 | PARA | 字符串 | 数据查询需要的参数，没有参数不需此选项 |
| 4 | LINK | 整数 | 增强安全性（可选） |

#### 4.2 查询应答

Web服务器收到查询请求后，验证信息，执行查询操作，然后返回结果。TYPE=2时表示查询应答，其他选项如表2-15。

表2-15 控制应答报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | RET | 整数 | 返回代码，-1表示请求失败；>=0表示查询成功的新消息数量。 |
| 2 | ID | 整数 | 如果查询ID时，具有此选项 |
| 3 | INFO | 字符串 | 错误原因：代码:错误原因（出错时）  未读消息代码（查询成功时有效） |

查询到有未读消息后，利用消息传递协议的未读消息请求进行消息传输的要求。

### 5、消息传递协议

#### 5.1 单个消息推送请求

消息推送请求是消息产生者（监控端或者web服务器）向消息接收者（web服务器或者登录到监控端的管理端）主动发送报警或者聊天消息。

1、推送请求

3、未读消息请求

2、推送应答

4、未读消息通知

5、获取消息应答

web

管理APP

前端设备

CMD=5表示消息推送请求协议；

单个消息推送协议，TYPE=1，其他选项如表2-16。

表2-16 消息推送请求报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | NUM | 整数 | 消息数量 |
| 2 | INFO | 字符串 | 消息体采用JSON数组格式，其关键字如下：  (USER, DEST, CLASS,DATE,CONTENT) |
| 3 | LINK | 整数 | 增强安全性（可选） |

INFO中的信息解析如下：

USER：消息产生者的ID

DEST：消息接收者ID：消息接收者ID（>10000）；接收者类别(<100)：

0 所有APP用户；1前端设备关联人；2 所有设备管理员；3 厂商设备用户

CLASS: 1报警消息；2聊天消息； 4系统通告 8 联系人通知消息 16 关联人通知

DATE：消息产生时间，一个整数值。

CONTENT：消息内容，CLASS不同而不同。

当CLASS=1时，由SORT类别和LEVEL级别和ATTTCH构成；

=2时，由MSG消息和TYPE字型、COLOR构成；

=4时，由TITLE标题、MSG消息、SET字符集构成。

=8时，由 KIND, MSG构成（仅用于服务器向APP推送消息）

=16时，由PUSER, KIND,RIGHT, PASS, MSG构成（仅用于服务器向APP推送消息）

PUSER 整数 关联的前端设备ID。

DATE 长整型 消息产生时间（毫秒）

KIND 字节型 报文子类别：0请求确认；1用户确认；2、用户否认；3 解除通知；4 添加通知（不需要用户确认）

RIGHT 字节型 权限代码：0管理权限；1操控权限；2查看权限；3接收权限；

PASS 字符串 设定的登录前端设备密码（当不允许登录或者脱离关联时，此项为null)

MSG 字符串 留言信息

#### 5.2 消息推送应答

消息接收者收到请求后，给出应答。TYPE=2，其他选项如表2-17。

表2-17 消息推送应答报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | RET | 字符串 | 返回代码，-1表示请求失败；0表示请求成功。 |
| 2 | INFO | 字符串 | 错误原因或“OK”。 |

#### 5.3 获取未读消息请求

APP用户向web服务器或者前端设备请求获取未读消息。当某个APP获知有未读消息时，主动向服务器请求未读消息。TYPE=3，其他选项如表2-18。

表2-18 未读消息请求报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | CLASS | 字节型 | 消息类型。0表示所有类型。 |
| 2 | NUM | 整数型 | 表示可以读取消息数量，为0表示由发送方自动封装 |
| 3 | LINK | 整数 | 增强安全性（可选） |

#### 5.4 未读消息通知

当收到APP的未读消息请求，或者用户在线时，由于收到消息推送要传递到该用户，或者定时器查询到该用户有未读消息，都需要使用本协议让web服务器向APP用户通告有未读消息。TYPE=4，其他选项如表2-19。

表2-19 未读消息通告报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | NUM | 整数 | 消息数量 |
| 2 | SIGN | 整数 | 特征码，用于查找消息是否重复或者状态置位标记 |
| 3 | INFO | 字符串 | 消息体，用JSON数组表示。内容如下：  ((USER, CLASS, DATE, CONTENT), |

消息体INFO中的各个域含义和TYPE=1的描述一样。

SIGN用于APP判断收到的信息是否最新的未读消息。（可能因为应答丢失，导致web服务器重发与以前一样的未读消息通知）。

#### 5.5 获取消息应答

APP用户向web服务器应答收到未读消息，web服务器收到以后，对相关信息的数据表进行操作，以后该用户不再有此未读消息。TYPE=5，其他选项如表2-21。

Web服务器通过SIGN对APP收到的各个消息状态进行标记，标记为已读。

表2-21 获取消息应答报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | RET | 整数 | 返回代码，0表示正确收到信息；1 重复收到；-1表示失败 |
| 2 | INFO | 字符串 | RET = -1：错误原因  RET=其他值：SIGN值 |

### 6、局域网发现协议

当管理APP连接上wifi时，主动刷新或者每60秒向局域网发送一个广播，通告自己的帐号信息。当有监控端（前端设备）收到此信息时，如果发现此用户帐号没有在本监控端登录，向管理APP发送一个应答信息。

1广播通报

2、前端设备应答

管理APP

前端设备

CMD=6表示局域网发现协议；

#### 6.1 局域网广播通告报文

局域网广播通告报文由管理APP发出。要执行此操作，管理APP当前上网模式必须是wifi。管理APP根据设定按时发送局域网广播通报报文，也可以让用户点击刷新人工要求发送此报文。TYPE=1，其他选项如表2-22。

表2-22 局域网广播通告报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | USER | 字符串 | 广播者帐号，8-20个字符 |

#### 6.2 前端设备应答报文

前端设备收到广播后，如果发现该帐号没有登录到该前端设备上，且设置了可以应答，则给出应答。TYPE=2，其他选项如表2-23。

表2-23 前端设备应答报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | INFO | 字符串 | 前端设备帐号。 |
| 2 | RET | 整数 | 与管理APP关系代码：0管理权限；1配置权限；2查看权限；3接收权限； -1 没有关系。 |

注：前端设备可以配置是否允许响应局域网发现报文。

### 7、文件信息传输协议

文件信息传输协议内含支持使用带内UDP停等协议和带外使用其他协议实现，如FTP、HTTP等。带内UDP文件信息传输的效率比较低，但是实现简单。

传输文件场合：下载插件，下载程序升级，下载报警附件，下载图片，下载视频文件等

1文件传输请求

2、文件传输应答

2、文件传输应答

1文件传输请求

2、文件传输应答

3终止文件传输

4文件信息请求

5 文件信息应答

前端设备或者Web

管理APP或前端设备

CMD=7表示文件信息传输协议；

#### 7.1 文件传输请求

所有文件传输需要接收方请求传输。系统先通过其他协议让接收方获得文件有关信息。然后提出文件传输请求。TYPE=1，其他选项如表2-24。

表2-24 文件传输请求报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | USER | 字符串 | 请求者帐号，8-20个字符 |
| 2 | FILE | 字符串 | 文件URL |
| 3 | SIZE | 整数 | 请求大小 |
| 4 | FROM | 整数 | 起始位置 |
| 5 | INDEX | 整数 | 支持的传输方式：0带内编码；1带内二进制；2 ftp；4 http；8 ftp服务器中转；16 http服务器中转 |
| 6 | LINK | 整数 | 增强安全性（可选） |

对于比较大的文件，需要多个报文传输。如果一次请求的大小太大，一次传输过来的报文太多，可能丢包，接收方也需要很大的缓冲区。因此要求每个请求的SIZE<10KB。传输完一批数据，然后传输下一批，不要一次请求所有数据。

#### 7.2 文件传输应答

传输应答可以对同一个请求应答多次，这时每个应答报文的ACK应该是一致的。

TYPE=2，其他选项如表2-25。

表2-25 文件传输应答报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | RET | 整数 | 返回代码，-1表示请求失败；>0表示传输方式。 |
| 2 | INFO | 字符串 | (RET=-1)：错误原因  (RET=其它)：本次传输累计传输总长度 |
| 3 | LEN | 整数 | 本次传输实际内容长度 |
| 3 | CONTENT | 字符串 | RET=0：具体传输内容，用BASE64编码。  RET=1：CONTENT=OK，报文后面二进制文件信息。  RET=2,4：CONTENT=端口号；  RET=8,16：CONTENT=IP地址； |

失败的原因可能有文件不存在，请求的位置或者大小不符合要求等。

#### 7.3 终止文件传输

在文件传输过程中，如果需要传输方停止传输，可以发送此报文。TYPE=3，其他选项如表2-26。

表2-26 中止文件传输报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | USER | 字符串 | 请求者帐号，8-20个字符 |
| 2 | FILE | 字符串 | 文件URL |
| 3 | LINK | 整数 | 增强安全性（可选） |

#### 7.4 文件信息请求

需要请求文件的各种信息，比如大小和MD5等，可以发送此请求。TYPE=4，其他选项如表2-27。

表2-27 文件信息请求报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | FILE | 字符串 | 文件URL |
| 2 | TYPE | 整数 | 文件类型 0管理APP；1前端设备的程序；2前端设备插件；3前端设备动态库；  4 报警附件；5日志文件；6 配置文件；7多媒体文件；8其他； |

#### 7.5 文件信息应答

回答的文件信息，包括大小和MD5摘要值。TYPE=5，其他选项如表2-28。

表2-28 文件信息应答报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | RET | 整数 | -1表示错误；0表示成功。 |
| 2 | INFO | 字符串 | RET=0：JSON格式文件信息（FILE, SIZE, MD5)  RET=-1：错误码:错误原因 |

### 8、加密通信协议

加密协议由通信的主动方发起，先协商加密方法和临时通信密码组，然后再通信过程中，随机选择一个临时密码进行加密处理。临时密码组最多可以有32组密码，由首部扩展选项keyseq指定本报文及以后报文选择的临时通信密码。加密时，仅对DATA域的信息进行加密。

1加密通信请求

2、加密通信应答

管理APP/前端设备

前端设备/Web平台

CMD=8表示加密通信协议。

#### 8.1 加密通信请求

加密通信请求报文由作为客户端的管理APP或者前端设备发出，仅能够在登陆以后的某个时候开始。此报文可以重复请求，表示更新加密方法和密码组。TYPE=1，其他选项如表2-29。

表2-29 加密通信请求报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | USER | 字符串 | 广播者帐号，8-20个字符 |
| 2 | LINK | 整数 | 增强安全性（可选） |
| 3 | ENCRY | 整数 | 1 XOR；2 DES；4 IDEA；0取消加密。加密方法可以叠加，让对方选择一种。因此>0表示要求加密通信；=0表示取消加密通信 |
| 4 | NUM | 整数 | 临时密码组个数（和下面选项在Encry>0有效) |
| 5 | CIPHER | 字符串 | 临时密码组(NUMBER：PASSWORD)。采用JSON数组，并用用户密码加密后，再用BASE64编码传输。其中NUMBER部分是以后通信时，由KEYSEQ选项指定的值。 |

#### 8.2 加密通信应答

服务端收到请求后，验证客户的登录状态，记录客户的加密能力和选项，并报告客户本次通信选择的加密方法。TYPE=2，其他选项如表2-30。

表2-30 前端设备应答报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | RET | 整数 | -1表示错误；0表示成功。 |
| 2 | INFO | 字符串 | RET=0：选择的加密方法  RET=-1：错误原因 |

### 9、关联管理协议

关联人管理主要是对前端设备设置各种关联人。其方式包括前端设备本地Web配置、前端设备被具有管理功能的管理APP设置、APP通过web平台进行设置等。其中后两种方式需要协议支持。其具体情形如下：

1、关联帐号请求

1、关联帐号请求

2、关联帐号应答

2、关联帐号应答

3、脱联帐号请求

9、关联同步请求

Web转发

4、脱联帐号应答

10、关联同步应答

7、关联确认/脱联通知请求

3脱联帐号请求

8、关联确认/脱联通知应答

4脱联帐号应答

6、获取关联人应答

5、获取关联人请求

6、获取关联人应答

5、获取关联人请求

管理APP

管理APP

Web平台

前端设备

账号关联是在管理APP帐号和前端设备帐号之间建立一个管理关系。建立这个关系有5种方式，即在前端设备上本地设置关联人、管理关联人在前端设备上分享设备给其他人、一般管理APP用户自我申请（局域网发现后自我申请或者扫描设备二维码后自我申请）、管理关联人在Web平台上分享设备、一般管理APP用户通过Web平台申请成为关联人。

此外关联人自己或管理关联人还可以变更关联信息，比如密码、设备别名、关联权限等

不同方式下的关联帐号请求执行的流程具有差异，如表2-31所示：

表2-31 关联帐号请求处理要求

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 5种情况 | 适应场合 | 需前端设备或者管理关联人确认 | 需要被关联人确认 | 同步处理时机 |
| 前端设备本地设置关联人 | 前端设备上配置操作 | 不需要 | 需要 | 先同步到web平台，然后让被关联用户确认。 |
| 设备管理员通过前端设备分享 | 登录前端设备后操作 | 不需要 | 需要 | 先同步到web平台，然后让被关联用户确认。 |
| 设备管理员在web平台上分享 | 登录web平台后进行操作 | 不需要 | 需要 | 被关联人确认后同步到前端设备 |
| 关联人在前端设备上自我申请 | 在局域网内自动发现或扫描二维码添加 | 在前端设备配置确认或者登录设备或者平台的管理员确认 | 不需要 | 确认前后与web平台同步 |
| 关联人在Web平台上自我申请 | 通过Web平台申请关联 | 设备管理员登录Web平台或者前端设备时确认 | 不需要 | 确认前后与web平台同步 |

CMD=9表示关联管理协议；所有确认可以在前端设备和web平台上配置为自动确认。

#### 9.1 关联帐号请求

目前系统规定，一个监控设备最多只关联10个管理帐号。共有5种关联方式，除了前端设备本地配置以外，其他四种情况又分两大类，即管理关联人分享关联和自我申请关联。TYPE=1，其他选项如表2-32。

表2-32 关联帐号请求报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | REF | 布尔型 | 1表示管理员分享0表示自我申请 |
| 2 | USER | 字符串 | 申请者帐号，8-20个字符 |
| 3 | MUSER | 字符串 | 管理关联人帐号，8-20个字符。（自我申请时不需要此选项） |
| 4 | PUSER | 字符串 | 前端设备帐号，8-20个字符 |
| 5 | ALIAS | 字符串 | 设备别名，可为空。8-20个字符 |
| 6 | RIGHT | 字节型 | 权限代码：0管理权限；1操控权限；2查看权限；3接收权限。 |
| 7 | PASSWORD | 字符串 | 设置前端设备关联人的访问密码 |
| 8 | LINK | 整数 | 申请者的登录连接号 |

管理关系目前仅支持四类，其中权限3以外的权限都需要设置登录前端设备密码。

#### 9.2 关联帐号应答

Web服务器或者前端设备收到关联帐号请求报文后，检查相应帐号是否存在，然后更正数据库后给出应答报文。由于所有的申请都需要确认。因此此应答仅表示信息被接收，而不是被确认了。所有关联关系在数据库中应有一个状态位分别标明等待确认、已经确认和已经否认。TYPE=1，其他选项如表2-33。

表2-33 关联帐号应答报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | RET | 整数 | 返回代码，0表示等待确认；-1表示关联帐号失败；1表示帐号已经存在关联关系或者自动确认。 |
| 2 | INFO | 字符串 | 错误原因、时间，当RET=-1时为错误原因；当RET>=0时为关联帐号成功的时间（毫秒数） |

#### 9.3 脱联帐号请求

脱联帐号是在管理帐号和监控帐号之间解除一个管理关系，由关联人本身、或者管理关联人提出，也可以在前端设备本地进行设置，这时仅需要进行同步到web平台即可。脱联申请不需要确认，但是要给相关关联人发出通知信息。TYPE=3，其他选项如表2-34。

表2-34 脱联帐号请求报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | REF | 布尔型 | 1表示管理员提出0表示自我申请 |
| 2 | USER | 字符串 | 申请者帐号，8-20个字符 |
| 3 | MUSER | 字符串 | 管理关联人帐号，8-20个字符。（自我申请时不需要此选项） |
| 4 | PUSER | 字符串 | 前端设备帐号，8-20个字符 |
| 5 | LINK | 整数 | 申请者的登录连接号 |

需要检查MUSER是否管理关联人，USER是否和PUSER有关联。

#### 9.4 脱联帐号应答

Web平台或者前端设备收到脱联帐号请求报文后，检查相应帐号是否存在，并具有相应权限，然后更正数据库给出确认报文。如是管理关联人申请的，还需要通知被解除关联的关联人。TYPE=4，其他选项如表2-35。

表2-35 脱联帐号应答报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | RET | 整数 | 返回代码，0表示通过脱联；-1表示脱联联帐号失败；1表示帐号已经脱联。 |
| 2 | INFO | 字符串 | 当RET=-1时为错误代码:错误原因；>=0时为脱联帐号成功的时间 |

#### 9.5 获取关联帐号请求

获取关联帐号的申请者是监控帐号获取所有在该前端设备上的管理关联人，他可以查看一个前端设备的所有关联人帐号，或者他所管理的所有监控设备列表。可以直接获取登录的前端设备上的信息，或者从平台获取他所管理的关联帐号信息。TYPE=5，其他选项如表2-36。

表2-36 获取关联帐号请求报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | USER | 字符串 | 申请者帐号，8-20个字符 |
| 2 | KIND | 字节型 | 获取类别：0、所有关联的前端设备帐号；1、获取某个前端设备上的所有管理关联人帐号；2、获取前端设备上所有关联人帐号。 |
| 3 | PUSER | 字符串 | 前端设备帐号，8-20个字符（仅当KIND为1、2时，且没有登录前端设备时有效） |
| 4 | LINK | 整数 | 申请者的登录连接号 |

使用时需要检查USER权限和登录连接号

#### 9.6 获取关联帐号应答

Web或者前端设备得到获取关联帐号请求报文后，检查相应帐号是否存在并登录，并具有相应权限，然后给出查询结果。TYPE=6，其他选项如表2-37。

表2-37 获取关联帐号应答报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | RET | 整数 | 返回代码，-1表示请求失败；n表示获得帐号数量。 |
| 2 | INFO | 字符串 | 当RET=-1时为错误原因；  RET>0时为获取帐号的信息，采用JSON数组格式  JSON关键字为ACCOUNT、RIGHT |

#### 9.7 关联确认/脱联通知等请求

本报文主要用来进行关联或者解除关联的信息确认，用于APP用户在确认后发给Web平台。如果web服务器收到信息后通知APP，或者web服务器的定时器定时发送给APP的，通过协议5进行。当添加或者删除关联的时候，需要通知管理关联人或者被关联本人确认或者知晓，这时候采用协议5进行通告。而APP确认的结果则通过此报文传递。TYPE=7，其他选项如表2-38。

表2-38 关联确认/脱联通知请求报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1. | REF | 布尔型 | 管理员还是普通的关联者 |
| 2 | PEER | 整数 | 通信对方的ID（批准者或者请求者） |
| 3 | PUSER | 整数 | 前端设备 |
| 4 | KIND | 字节 | 0请求关联 1确定关联 -1 否定或者脱联确定 |
|  | RIGHT | 字节型 | 权限代码：0管理权限；1操控权限；2查看权限；3接收权限；（当KIND为-1时没有此项） |
|  | PASS | 字符串 | 设定的登录前端设备密码（当KIND为-1，没有此项) |
|  | MSG | 字符串 | 留言信息（当KIND为-1时没有此项） |

#### 9.8 关联确认/脱联通知应答

收到请求信息后，Web服务器立即给予确认。然后利用协议5通知相关APP用户。TYPE=8，其他选项如表2-39。

表2-39 关联确认/脱联通知应答报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | RET | 整数 | 返回代码，0表示信息正确接收；1 重复接收；-1表示失败 |
| 2 | INFO | 字符串 | RET = -1：错误原因  RET=其他值：SIGN值 |

#### 9.9 关联同步请求

前端设备或者web平台设置关联关系之后需要双方保持一致，这时需要进行同步。关联同步发生的时机如下：如果前端设备登录了web平台，前端设备上的任何变更及时发送给web平台同步；Web平台上的关联变更也及时发送给前端设备同步；如果前端设备没有登录Web服务器，则当前端设备登录Web平台之后，立即进行一次同步。登录同步时，前端设备和web服务器都要检查在前端设备未登录平台期间是否发生了关联关系变化，因此，前端设备离线和上线时间需要记录，每次设置关联人的信息也需要记录时间。

此外，前端设备可以根据设置，强制获取Web平台的关联信息或者强制Web平台接收前端设备的关联信息。TYPE=9，其他选项如表2-40

表2-40 关联同步请求报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | USER | 字符串 | 前端设备帐号，8-20个字符 |
| 2 | KIND | 字节型 | 同步类型：1 设备要求平台对比；2 设备强制平台更新；3 设备请求平台信息；11 平台要求设备对比；12 平台要求设备更新；13 平台请求设备信息 |
| 4 | INFO | 字符串 | 要求对方强制更新或者对比时，传递到对方的关联人信息，采用JSON数组格式，内容如下：  ((关联人帐号ACCOUNT，权限RIGHT，别名ALIAS，密码PASS，设置日期时间TIME，状态STATE)，.......)  表中的密码为0表示不许登录设备  状态含义：0待审核，1通过，-1拒绝  同步成功后，平台或者设备删除状态为-1的关联人  KIND为3或者13时，没有此选项 |

#### 9.10 关联同步应答

Web平台或者前端设备收到关联同步报文后，根据KIND内容进行更新或者给出回答。TYPE=10，其他选项如表2-41。

表2-41 关联同步应答报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | RET | 整数 | 返回代码，-1表示请求失败；n表示获得的关联信息数量，0表示没有INFO信息。 |
| 2 | INFO | 字符串 | 当RET=-1时为错误信息：代码:错误原因  >0时为获取关联信息，具体信息内容如上表所述 |

#### 9.11 变更关联信息请求

所有关联人和前端设备的关联信息可以修改密码和别名。管理关联人还可以修改关联权限。如果修改的其他关联人权限、密码和别名，需要发送通知报文给相关关联人。TYPE=11，其他选项如表2-42。

表2-42 变更关联信息请求报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | REF | 布尔型 | 1表示管理关联人变更 0表示自己变更 |
| 2 | USER | 字符串 | 申请者帐号，8-20个字符 |
| 3 | MUSER | 字符串 | 管理关联人帐号，8-20个字符。（自我申请时不需要此选项） |
| 4 | PUSER | 字符串 | 前端设备帐号，8-20个字符 |
| 5 | KIND | 变更类别 | 1别名 2密码 4 权限 |
| 6 | ALIAS | 字符串 | 新别名（KIND&1为真时有此选项） |
| 7 | PASS | 字符串 | 新密码（KIND&2为真时有此选项） |
| 8 | RIGHT | 字符串 | 新权限（KIND&4为真时有此选项） |
| 9 | LINK | 整数 | 申请者的登录连接号 |

#### 9.12 变更关联信息应答

变更成功应答以后，如果是管理关联人变更其他关联人，需要发送通知报文。然后前端设备或者web平台需要进行信息同步。TYPE=12，其他选项如表2-43。

表2-43 变更关联信息应答报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | RET | 整数 | 返回代码，-1表示请求失败；0表示变更成功。 |
| 2 | INFO | 字符串 | RET=-1时为错误代码:错误原因（成功时不需要此项） |

### 10、联系人管理协议

联系人管理主要是让管理APP设置各种联系人，便于某设备的管理关联人将这些联系人设置为某设备的关联人，或者对其他联系人分享报警信息，进行安全交流，或者求救等。具体工作有如下几种情形：

a、系统通知消息

1、联系人添加请求

2、联系人添加应答

a、系统通知应答

3脱离联系请求

7、联系人通告/确认请求

4脱离联系应答

8、联系人通告/确认应答

5、获取联系人请求

6、获取联系人应答

9、变更联系人信息请求

管理APP

10、变更联系人信息应答

管理APP

Web平台

CMD=10表示联系人管理协议；添加联系人的确认可以人工配置自动确认。

#### 10.1 联系人添加请求

任何管理APP的帐号都可以添加为其他管理APP的联系人。添加过程和添加QQ好友没有区别。目前添加联系人之前，必须知道对方的帐号（今后可以提供模糊查询功能）。TYPE=1，其他选项如表2-44。

表2-44 联系人添加请求报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | USER | 字符串 | 申请者帐号，8-20个字符 |
| 2 | CUSER | 字符串 | 添加联系人帐号，8-20个字符 |
| 3 | ALIAS | 字符串 | 联系人别名，可为空，8-20个字符 |
| 4 | GROUP | 字符串 | 所属组名，可为空，8-16个字符 |
| 5 | MESSAGE | 字符串 | 留言 |
| 6 | LINK | 整数 | 申请者的登录连接号 |

#### 10.2 联系人添加应答

Web平台收到联系人添加请求报文后，检查相应帐号是否存在，然后更正数据库，然后给出确认报文。由于所有的申请根据配置有些需要确认，因此此确认有些仅表示信息被接收，而不是被确认了。联系人状态应有一个状态位标明等待确认、已经确认和已经否认。TYPE=2，其他选项如表2-45。

表2-45 联系人添加应答报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | RET | 整数 | 返回代码，0表示等待确认；-1表示关联帐号失败；1表示帐号已经关联过。 |
| 2 | INFO | 字符串 | 错误原因、时间，当RET=-1时为错误原因；当RET>=0时为关联帐号成功的时间 |

#### 10.3 脱离联系请求

脱离联系是解除两个联系人之间的关系，由两个联系人的任意一方提出。脱离联系申请不需要确认，但是要给相关联系人发出通知信息。此外，目前脱离联系并不删除所管理设备的关联，仅从双方的联系人中去掉。TYPE=3，其他选项如表2-46。

表2-46 脱离联系请求报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | USER | 字符串 | 申请者帐号，8-20个字符 |
| 2 | CUSER | 字符串 | 联系人帐号，8-20个字符 |
| 3 | LINK | 整数 | 申请者的登录连接号 |

#### 10.4 脱离联系应答

Web平台收到脱离联系请求报文后，检查相应帐号是否存在，然后更正数据库给出确认报文。并通知对方联系人。TYPE=4，其他选项如表2-47。

表2-47 脱离联系应答报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | RET | 整数 | 返回代码，0表示通过脱联；-1表示脱联联帐号失败；1表示帐号已经脱联。 |
| 2 | INFO | 字符串 | 当RET=-1时为错误代码:错误原因；>=0时为脱联帐号成功的时间 |

#### 10.5 获取联系人请求

获取联系人一般是在管理APP登录平台的时候。如果联系人很多，可能需要多个报文请求。TYPE=5，其他选项如表2-48。

表2-48 获取联系人请求报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | USER | 字符串 | 申请者帐号，8-20个字符 |
| 2 | FROM | 字节型 | 请求传输的序号。 |
| 3 | LINK | 整数 | 申请者的登录连接号 |

#### 10.6 获取联系人应答

Web平台每次从请求的序号开始传输（服务器可以将所有联系人保存在内存中供管理APP一次次请求后依次传输）。TYPE=6，其他选项如表2-49。

表2-49 获取联系人应答报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | RET | 整数 | 返回代码，-1表示请求失败；n表示还未读取联系人信息总数量。 |
| 2 | NUM | 整数 | 本次传输的联系人信息数量，最大为40个。如果小于40，表示本次已经将联系人信息读取完成。 |
| 3 | INFO | 字符串 | 当RET=-1时为错误原因；  RET>0时为获取帐号信息，JSON数组表示：帐号ACCOUNT，别名ALIAS，组名GROUP |

#### 10.7 联系人通告/确认请求

当添加或者删除联系人的时候，需要通知有关联系人，并由联系人确认。需要其本人确认或者知晓，使用协议5进行系统通知。用户确认的结果则通过本报文传递给Web服务器。TYPE=7，其他选项如表2-50。

表2-50 联系人通告确认请求报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | LINK | 整数 | 用户的登录连接号 |
| 2 | USERID | 整数 | 被关联用户ID |
| 3 | KIND | 字节 | 0确认 1确定 -1 否定 |
| 3 | MSG | 字符串 | 消息体，备注留言 |

#### 10.8 联系人通告/确认应答

收到请求信息后，立即给予确认。TYPE=8，其他选项如表2-51。

表2-51 联系人通告确认应答报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | RET | 整数 | 返回代码，0表示信息确认；-1表示失败 |
| 2 | INFO | 字符串 | 出错时的错误代码或者正确时的SIGN |

#### 10.9 变更联系人信息请求

联系人的别名和组名是可以修改的。修改后的信息需要保存在Web平台。TYPE=9，其他选项如表2-52。

表2-52 变更联系人信息请求报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | USER | 字符串 | 申请变更的联系人帐号，8-20个字符 |
| 2 | KIND | 变更类别 | 1别名 2组名（可以叠加） |
| 3 | ALIAS | 字符串 | 新别名（KIND&1为真时有此选项） |
| 4 | GROUP | 字符串 | 新组名（KIND&2为真时有此选项） |
| 5 | LINK | 整数 | 申请者的登录连接号 |

#### 10.10 变更联系人信息应答

TYPE=10，其他选项如表2-53。

表2-53 变更联系人信息应答报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | RET | 整数 | 返回代码，-1表示请求失败；0表示变更成功。 |
| 2 | INFO | 字符串 | 当RET=-1时为错误代码:错误原因（成功时不需要此项） |

### 11、升级查询协议

升级查询协议是管理APP、前端设备的程序、插件、动态库等需要定时更新时对服务器的查询操作，主要包括查询请求和查询应答两类操作。每小时查询一次。

1、升级查询请求

2、升级查询应答

web服务器

管理APP/前端设备

#### 11.1 升级查询请求

升级查询请求是客户向web服务器平台发送的查询命令，该命令可在非登录状态下应用，因此不检查用户是否登录。处理时，需要检查用户的权限，查看是否有更新权限设置。

CMD=11表示控制协议；TYPE=1时，其他选项如表2-54。

表2-54 升级查询请求报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | USER | 字符串 | 用户账号 |
| 1 | SERIAL | 字节型 | 请求查询程序类型码：0管理APP、1前端设备的程序、2前端设备插件、3前端设备动态库 |
| 2 | VERSION | 字符串 | 程序当前版本号XXYYZZ |

#### 11.2 升级查询应答

web服务器收到升级请求后，检查是否有最新版本程序。并获取文件的URL。文件的具体信息通过文件信息查询协议获取。TYPE=2，具体表项说明如下。

表2-55 升级查询应答报文选项表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 字段 | 类型 | 描述 |
| 1 | RET | 整数 | 返回代码，-1表示请求失败；0表示已经是最新版本；n>0表示存在n个新版本。 |
| 2 | INFO | 字符串 | RET=-1: 错误原因，格式：错误代码:错误信息  RET =0: 当前版本号信息。  RET > 0: 当前最新版本信息，JSON格式表示。  新版本号VERSION，文件名URL |

**附一：常见错误编码及错误原因**

1:报文格式错误

2:有不能识别的选项

3:权限不够

4:帐号不存在

5:账号没有登录

6:账号重复

7:没有要求的文件

8:请求超过

9:不存在的代码

10:不识别的命令

11:要求的信息不存在

12:已达上限

13:不支持的文件传输方式

......

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 协议名称 | 功能 | 通知界面 | 后处理 | 定时启动  任务列表 | 处理要点 | 重发 | 消息编号 | | |
| 请求 | 通知栏 | 通知activity |
| 连通测试0 | 连通测试 |  |  |  |  |  | 10 ConnectMsg |  | 10通知结果 |
| 连接管理协议1 | 登录 | 是 | 启动保活,数据查询 | 是 | 区分登录设备或者平台，登录后界面有显示 | 是 | 11 ConnectMsg |  | 11结果通知：APP |
| 登出 | 是 | 禁止保活 |  | 不用重发，取消所有网络操作。退出前自动进行 |  | 12 ConnectMsg |  | 12结果通知：APP |
| 保活 | 离线通知 |  | 是 | 不用重发 |  | 27 |  | 27状态变化通知：APP |
| 平台帐号管理2 | 注册 | 是 |  |  | 在登陆之前进行 | 是 | 13 RegisterMsg |  | 13 结果通知 |
| 修改 | 是 |  |  | 修改用户名和密码要重修登录 | 是 | 14 RegisterMsg |  | 14结果通知：APP |
| 注销 | 是 |  |  | 需要重新登录 | 是 | 15 RegisterMsg |  | 15结果通知：APP |
| 控制协议3 | 控制 | 是 |  |  | 必须在登陆设备后进行 | 是 | 16 ControlMsg |  | 16 结果通知：+ConRetMsg |
| 数据查询4 | 查询 | 是 | 请求消息 |  | 可以查询设备和平台，登录后立即进行 | 是 | 1 QueryMsg | 1 消息通知 | 1 结果通知+数据库 |
| 消息推送5 | 消息通知 |  |  |  | 处理后立即请求消息 |  |  |  |  |
| 请求消息 | 是 |  |  | 主要是获取未读消息 | 是 | 2 GetMsg | 2 消息通知 | 2 结果通知+数据库 |
| 局域网发现6 | 局域网发现 | 是 |  |  | 与是否登录无关 | 是 | 3 ConnectMsg | 3 发现通知 | 3 结果通知 |
| 文件传输7 | 文件传输 | 是 | 请求安置 | 是 | 事先获得文件的类型和MD5，然后下载。 | 是 | 4 FileMsg | 4安装通知 | 4 结果通知+FileRetMsg |
| 加密协议8 | 加密 |  |  |  | 目前未处理 | 是 | 26 EnCodeMsg |  |  |
| 关联管理9 | 关联账号 | 是 |  |  | 登录后处理，配合界面和数据库 | 是 | 17 RelaterMsg |  | 17 结果通知+数据库 |
| 脱联账号 | 是 |  |  | 登录后处理，配合界面和数据库 | 是 | 18 RelaterMsg |  | 18 结果通知+数据库 |
| 获取关联 | 是 |  |  | 登录后处理，配合界面和数据库 | 是 | 19 RelaterMsg |  | 19 结果通知+数据库 |
| 通告确认 | 是 |  |  | 登录后处理，配合界面和数据库 | 是 | 5RelaterMsg | 5 消息通知 | 5 结果通知+数据库 |
| 变更关联 | 是 |  |  | 登录后处理，配合界面和数据库 | 是 | 20 RelaterMsg |  | 20 结果通知+数据库 |
| 联系人管理10 | 添加联系 | 是 |  |  | 登录平台后处理，配合界面和数据库 | 是 | 21 ContactMsg |  | 21 结果通知+数据库 |
| 脱离联系 | 是 |  |  | 登录平台后处理，配合界面和数据库 | 是 | 22 ContactMsg |  | 22 结果通知+数据库 |
| 获取联系 | 是 |  |  | 登录平台后处理，配合界面和数据库 | 是 | 23 ContactMsg |  | 23 结果通知+数据库 |
| 变更联系 | 是 |  |  | 登录平台后处理，配合界面和数据库 | 是 | 24 ContactMsg |  | 24 结果通知+数据库 |
| 通告确认 | 是 |  |  | 登录平台后处理，配合界面和数据库 | 是 | 6 ContactMsg | 6 消息通知 | 6 结果通知+数据库 |
| 升级查询11 | 升级查询 | 是 | 请求下载 | 是 | 注意区别人工和自动行为 | 是 | 7 UpdateMsg | 7新版本通知 | 7结果通知+UpdateRetMsg |
| 网络状况 |  | 状况变化 | 下载管理 |  | 注册系统广播 |  |  |  | 25 变化结果通知+APP |
| 退出程序 |  | 请求 |  |  | 启动登出操作，关闭服务和线程等。 |  | 0 |  |  |

注：APP协议处理逻辑表

添加一个关联人的典型处理过程说明：（删除，前端设备添加等通知类似）

CMD=9,TYPE=1

①

说 明

1、管理APP请求某个APP关联一个前端设备

2、Web服务器记录数据库信息后，如果被关联的APP在线，立即发送一个通知；

3、如果用户没收到，定时器定时发送通知

4、用户如果不在线，在用户登录时，查询有未读通知，利用命令5-3来请求消息。

5、服务器在得知APP收到消息后，更改数据库状态，不再通知。

6、APP用户处理通知消息后，对消息做出回应。

7、Web服务器收到用户应答后，修改消息状态

8、Web服务器将用户的回应结果送给管理APP（这个过程和前面2、3、4类似，分三种情况）

9、Web服务器收到管理APP应答后，修改消息状态。然后不会再通知管理APP

10、Web平台在第7步以后，和前端设备同步关联人信息，让前端设备信息同步。

其他情况说明：

1、如果某个用户配置了自动添加，则不需要APP回应（上述第6步）

2、删除处理时，也不需要上述第6步。

3、普通APP自己请求关联时，过程与前述的一致

立即通知在线用户

CMD=9,TYPE=7

CMD=9,TYPE=2

CMD=9,TYPE=8

CMD=9,TYPE=7

定时通知在线用户

⑤

与前端设备同步

④

立即通知管理用户

③

②

用户响应通知应答

上线用户请求通知

CMD=9,TYPE=10

CMD=9,TYPE=9

CMD=9,TYPE=8

CMD=9,TYPE=7

CMD=9,TYPE=8

CMD=9,TYPE=7

CMD=9,TYPE=8

CMD=9,TYPE=7

CMD=5,TYPE=3

CMD=9,TYPE=8

普通APP

Web平台

前端设备

管理APP