目录

[第一章 概述 1](#_Toc390179589)

[1.1 背景 1](#_Toc390179590)

[1.1 协议简介 1](#_Toc390179591)

[第二章 协议规范 1](#_Toc390179592)

[2.1 协议流程 1](#_Toc390179593)

[2.2 报文格式 2](#_Toc390179594)

[2.2.1 客户端注册到前置服务器request 3](#_Toc390179595)

[2.2.2 客户端注册到前置服务器response 3](#_Toc390179596)

[2.2.3 客户端与ALLPASS服务器 3](#_Toc390179597)

[2.2.4 客户端注册到控制服务器request 3](#_Toc390179598)

[2.2.5 客户端注册到控制服务器response 4](#_Toc390179599)

[2.2.6 客户端反注册到前置服务器request 4](#_Toc390179600)

[2.2.7 客户端反注册到前置服务器response 5](#_Toc390179601)

[2.2.8 客户端发送心跳至心跳服务器request 5](#_Toc390179602)

[2.2.9 客户端发送心跳至心跳服务器response 5](#_Toc390179603)

[2.3 报文加密流程 6](#_Toc390179604)

[2.3.1 第一步 6](#_Toc390179605)

[2.3.2 第二步 6](#_Toc390179606)

[2.3.3 第三步 6](#_Toc390179607)

[2.3.4 第四步 6](#_Toc390179608)

[2.3.5 第五步 7](#_Toc390179609)

[2.4 报文解密流程 7](#_Toc390179610)

[2.4.1 第一步 7](#_Toc390179611)

[2.4.2 第二步 7](#_Toc390179612)

[2.4.3 第三步 7](#_Toc390179613)

第一章 概述

## 1.1 背景

## 1.2 协议简介

## 1.3 常用术语

|  |  |
| --- | --- |
| 关键字 | 描述 |
| 通信版本 | 决定报文填充内容，常用版本有1.0与2.0 |
|  |  |

第二章 协议规范

## 2.1 协议流程

前置服务器、控制服务器、心跳服务器监听的均为端口18000。

说明：

1. 客户端访问前置服务器，获取通信版本。
2. 前置服务器返回通信版本，返回的通信版本通常为1.0。之后所有的步骤则必须使用1.0的方式填充报文。
3. 客户端访问前置服务器，请求登陆所需资源.
4. 前置服务器返回相应的资源。
5. 客户端访问控制服务器请求登陆。
6. 控制服务器校验账号的有效性后，打开QQSG通道。
7. 控制服务器返回登陆结果。

8、反注册前置服务器，释放占用的资源。

9、返回释放队列结果，此时登陆操作完成。

10、注册心跳。

11、返回注册结果；如果不同主机使用同一个账号登陆，此处返回结果为refuse。

12、周期性的访问后置服务器和发送心跳包。

## 2.2 报文格式

认证交互流程的报文均使用TCP传输。

### 2.2.1 客户端与前置服务器交互通信版本request

因为此时还没有得到服务器的通信版本，如果是第一次开启客户端，默认的通信版本2.0进行交互。如果是客户端被注销，再重新登录，会使用通信版本1.0进行交互。

*报文格式*

报文分为head域与data域，head域使用红色框表示，data域使用橘色框表示。

HEAD：固定长度16byte，byte0填充0x01，代表query，byte1填充0x30，代表randomkey。

账号：客户端账号。

IP：客户端IP地址，格式为使用.分割。

MAC：客户端MAC地址，格式使用：分割。

密码：客户端密码。

VERSION：客户端版本，目前版本号为5.10。

填充数据：填充data域至512byte

### 2.2.2 客户端与前置服务器交互通信版本response

*报文格式*

报文分为head域与data域，head域使用红色框表示，data域使用橘色框表示。

HEAD：固定长度16byte，byte0填充0x02，代表accept，填充0x03，代表refuse；byte1填充0x30，代表randomkey。

填充数据：在偏移量496~498中填充了通信版本，这个版本则为以后客户端与服务器之间交互的通信版本号，其余数据均为乱码。

### 2.2.3 客户端注册到前置服务器request

通过访问前置服务器来获取其他的必要资源，，前置服务器在现实环境中有两台，地址为172.21.230.66与172.18.212.162。

*报文格式*

报文分为head域与data域，head域使用红色框表示，data域使用橘色框表示。

HEAD：固定长度16byte，byte0填充0x01，代表query，byte1填充0x02，代表register。

账号：客户端账号。

IP：客户端IP地址，格式为使用.分割。

MAC：客户端MAC地址，格式使用：分割。

填充数据1：填充304字节0x0。

VERSION：客户端版本，目前版本号为5.10。

填充数据2：填充data域至512byte。

### 2.2.4 客户端注册到前置服务器response

返回资源有9个，我们关注的只有控制服务器ip、心跳服务器ip、心跳间隔（通常为60），设备号（通常为1）。控制服务器与心跳服务器都不止一台，前置服务器会根据负载情况进行选择；设备号用于填充报文。

*报文格式*

报文分为head域与data域，head域使用红色框表示，data域使用橘色框表示。

HEAD：固定长度16byte，byte0填充0x02，代表accept，填充0x03，代表refuse；byte1填充0x02，代表register。

类型：有三种选择，TEXT、HTTP、SESM。实际中返回的应该是SESM。

资源：使用‘\t’作为分隔符，返回客户端资源，资源包括skurl,心跳ip,控制ip,消息ip,后置ip,allpass地址(以/结尾),是否采用控制

### 2.2.5 客户端注册到控制服务器request

控制服务器用户验证客户端账号密码的有效性，如果验证验证有效，便会开启qqsg通道。

*报文格式*

报文分为head域与data域，head域使用红色框表示，data域使用橘色框表示。

HEAD：固定长度16byte，byte0填充0x01，代表query，byte1填充0x02，代表register。

账号：客户端账号。

IP：客户端IP地址，格式为使用.分割。

MAC：客户端MAC地址，格式使用：分割。

密码：客户端密码。

VERSION：客户端版本，目前版本号为5.10。

DEVNO：设备号，由前置服务器返回，通常为1。

填充数据：填充data域至512byte。

### 2.2.6 客户端注册到控制服务器response

如果发生账号不存在、密码不正确等错误，返回结果会提示示ERROR并有提示消息

*报文格式*

报文分为head域与data域，head域使用红色框表示，data域使用橘色框表示。

HEAD：固定长度16byte，byte0填充0x02，代表accept，填充0x03，代表refuse；byte1填充0x02，代表register。

资源：使用‘\t’作为分隔符，返回客户端资源，资源包括版本号，是否dhcp，有效期，余额。但这里我们可以不用理会返回的信息，直接跳过即可。

填充数据：填充data域至512byte。

### 2.2.6 客户端反注册到前置服务器request

报文格式

报文分为head域与data域，head域使用红色框表示，data域使用橘色框表示。

HEAD：固定长度16byte，byte0填充0x01，代表query，byte1填充0x03，代表unregister。

账号：客户端账号。

IP：客户端IP地址，格式为使用.分割。

MAC：客户端MAC地址，格式使用：分割。

密码：客户端密码。

VERSION：客户端版本，目前版本号为5.10。

DEVNO：设备号，由前置服务器返回。

填充数据：填充data域至512byte。

### 2.2.7 客户端反注册到前置服务器response

报文分为head域与data域，head域使用红色框表示，data域使用橘色框表示。

HEAD：固定长度16byte，byte0填充0x02，代表accept，填充0x03，代表refuse；byte1填充0x03，代表unregister。

填充数据：填充data域至512byte。

### 2.2.8 客户端发送心跳至心跳服务器request

报文分为head域与data域，head域使用红色框表示，data域使用橘色框表示。

HEAD：固定长度16byte，byte0填充0x01，代表query，byte1填充0x02，代表register。

账号：客户端账号。

IP：客户端IP地址，格式为使用.分割。

MAC：客户端MAC地址，格式使用：分割。

LOG：测试客户端的特殊日志发送功能，填充字符串” LOG#00001:客户测试”。

COMPUTER ：默认填充值为1。

填充数据：填充data域至512byte。

### 2.2.9 客户端发送心跳至心跳服务器response

报文分为head域与data域，head域使用红色框表示，data域使用橘色框表示。

HEAD：固定长度16byte，byte0填充0x02，代表accept，填充0x03，代表refuse；byte1填充0x04，代表heartbeat。

填充数据：填充data域至512byte。

## 2.3 报文加密流程

### 2.3.1 第一步

橘色框表示data域，对data域中偏移量399~511中每个字节写入0~127中的随机数。

### 2.3.2 第二步

橘色框表示data域，如图所示，有5个选项被填入，用于客户端与服务器之间的加解密与认证，长度表示后面选项数据的字节长度。

Date：报文发送时间，格式为yyyymmdd

Vserion：通信版本号，目前版本是2.0，作为字符串被填入。

question：产生9个字符的字符串，每个字符为0~9的随机数。

Answver：通过question选项，算出question的md5值。

Pwd：该值当前应该为“zbn”。

### 2.3.3 第三步

以5个密钥为基础，对数据进行第一道加密操作。加密方法为，把数据以字节为单位，分别与密钥进行异或操作位运算。

然后再进行第二道加密，加密方法为第1位数字加4，第2位字母加5，数字奇数位加3，偶数位加1，字母奇数位加3，偶数位加1。

### 2.3.4 第四步

重复第三步的操作，只是这次加密对象时5个密钥本身。并且用于加密的密钥使用双方已经预定义好的key。

### 2.3.5 第五步

将加密后的密钥，分成两个部分，放在偏移量500~501字节和507~509字节。这样便得到最后的整个加密报文。

## 2.4 报文解密流程

### 2.4.1 第一步

从data域中偏移量500~501字节和507~509字节取出密钥。

### 2.4.2 第二步

对密钥进行第一道解密，解密方法为第1位数字减4，第2位字母减5，数字奇数位减3，偶数位减1，字母奇数位减3，偶数位减1。

再进行第二道解密，使用双发预定义好的可以，采用异或位操作，得到原始的密钥信息。

### 2.4.3 第三步

利用得到的原始密钥信息，重复第二步操作。得到解密后的完整报文信息。