★ 内部资料，敬请保密 ★

康泰物联网系统

外层协议说明

版本：1.1Beta

浙江欧佰信息技术有限公司　技术部

版本变更说明

版本号	发布时间	变更说明
1.0Beta	2014-10-31	1.0Beta 版
1.1Beta	2015-06-11	修改 T 口心跳，服务器额外返回当前时间给设备

1、协议概述

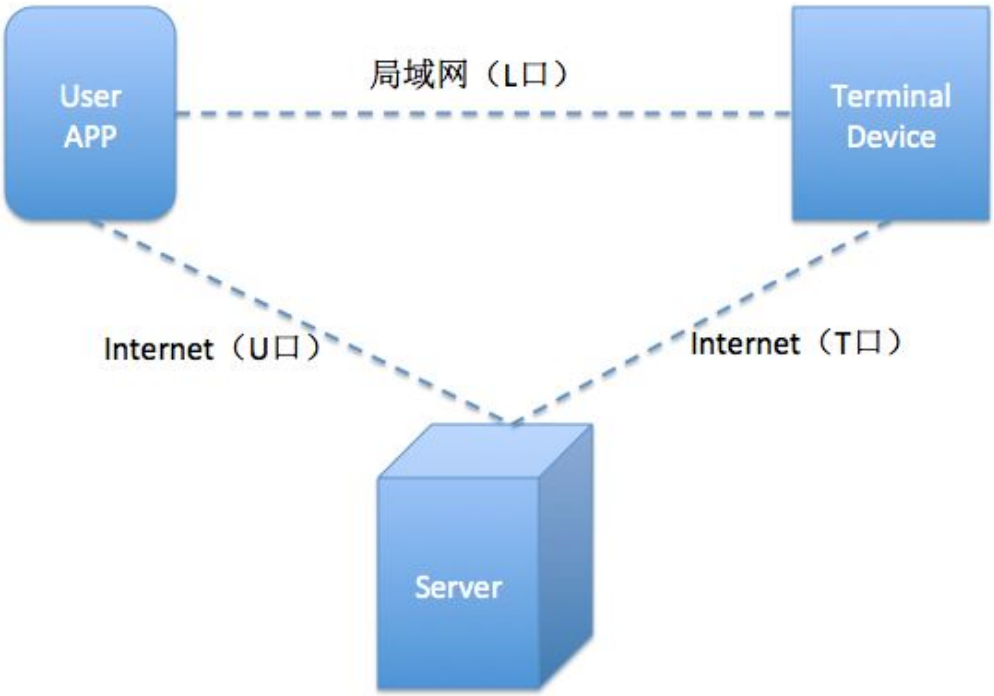
（1）物联网系统的通信协议，分成外层协议、内层协议 2 部分。

（2）该协议文档定义了外层协议部分的内容。需要结合《内层控制协议》进行开发。

（3）该协议内容由 3 部分组成：

- T 口协议——Terminal，WiFi 模块与服务器之间的协议，用于远程控制
- L 口协议——Local，WiFi 模块与手机 APP 之间的局域网协议，用于本地控制
- U 口协议——User，手机 APP 与服务器之间的协议，用于远程控制

  如下图所示：



（4）T 口、U 口使用 TCP 长连接；L 口使用 UDP 协议。

（5）该协议中的数据，如无特殊说明，均使用网络字节序。

（6）该协议中的命令返回参数 Result，统一使用 0x00 表示操作成功，其他值表示失败。

2、协议格式

T 口、L 口、U 口，无论 TCP 和 UDP，均使用如下的协议数据格式：

PV	Flag	MAC			
Len	Reserved	协议序号	厂家代码	授权码	设备类型
Data（内层协议数据）					
……					

2.1 协议格式说明

其中，每部分的含义如下：

- PV——1 字节，协议版本（Protocol Version），目前定为 0x01
- Flag——1 字节，其中：

  Bit 0：预留，请置 0

  Bit 1：发起/回复命令，0-发起，1-回复

  Bit 2：是否已设置管理员，0-未设置，1-已设置。如果是无管理员系统设备，则置 1 表示设备锁定，0 为非锁定状态。

  Bit 3：预留，请置 0

  Bit 4：预留，请置 0

  Bit 5：预留，请置 0

  Bit 6：是否加密，0-表示没有加密，1-数据从 Reserved 位（包括）开始至内层协议结束进行加密（上图阴影部分）。

  Bit 7：预留，请置 0
- MAC——6 字节，MAC 地址。
- Len——1 字节，阴影部分数据的长度。如果对阴影部分进行了加密，则是阴影部分数据加密后的长度。
- Reserved——1 字节，保留字节，请置 0x00。
- 协议序号——2 字节，发送方每发一次数据包将此值自加，回复方原值返回，溢出后归零继续自加，用于区分同一协议多次发送，以及数据包发送顺序。
- 厂家代码——1 字节，用于标志设备的厂家信息。
- 授权码——2 字节，用于验证服务授权。
- 设备类型——1 字节，用于标志设备类型。
- Data——可变长度字节，由 Len 字节可确定其实际长度。

具体的设备类型、授权码，请参照《内层控制协议》中的定义。

2.2 加密机制说明

康泰物联网系统使用 AES128 CBC 方式加密，使用 PKCS5Padding 算法进行补位。密钥和 IV 使用相同的值。

默认密钥：保密数据，另行告知。

在 Device 未得到 Server 分配的随机密钥之前，APP 未得到 Device 分配的随机密钥之前，APP 未得到 Server 分配的随机密钥之前，均使用默认密钥进行加密。

2.3 协议命令说明

内层协议数据的第 1 个字节为协议命令。协议命令长度为单字节，低 5 位用于表示命令号，高 3 位用于表示此条协议的类型。

Bit7	Bit6	Bit5	说明
0	0	0	设备专用控制协议
0	0	1	L 口专用协议
0	1	0	T 口专用协议
1	0	0	U 口专用协议
0	1	1	T/L/U 口公共协议

其中，T 口专用协议、U 口专用协议，由 Server 立刻返回。而设备专用控制协议、公共协议，如果发往 Server 的话，则由 Server 进行透传转发，Server 并不会立刻返回数据（0x61 心跳命令除外）。

3、T 口专用协议

3.1 0x41 获取工作服务器(TCP)

Device Request: | 41 |

Server Response: | 41 | IP Address | Port |

参数说明：

IP Address（4 - Byte）和端口号（2 - Byte）用于服务器分布式部署时的模块访问重定向、负载均衡等

Key Len：1 - Byte，密钥长度

Key：用于对之后的协议进行加密所用的密钥，密钥为服务器随机生成回复给 Device，目前暂定 IV 和 Key 值相同

命令说明：

该命令是设备与负载均衡服务器进行通信。设备与某一工作服务器建立 TCP 连

接之前，均需要发送该命令，获取工作服务器的 IP 和端口。
负载均衡服务器的 IP 和端口，请参照具体项目的《内层控制协议》中的定义。
发送该命令时，如果加密，请使用默认的密钥。

3.2 0x42 请求接入(TCP)

Device Request: | 42 |
Server Response: | 42 | Key Len | Key |
参数说明：

Key Len：1 - Byte，密钥长度

Key：用于对之后的协议进行加密所用的密钥，密钥为服务器随机生成回复给 Device，目前暂定 IV 和 Key 值相同

命令说明：
设备与某一工作服务器建立 TCP 连接之后，首先需要发送该命令，以便获取密钥数据。如果连接断开，重新建立 TCP 连接，则需要重新发送该命令。
发送该命令时，如果加密，请使用默认的密钥。

3.3 0x43 设备恢复出厂设置(TCP)

Device Request: | 43 | FF FF FF FF |
Server Response: | 43 | 55 55 55 55|
参数说明：

请求：固定为 4 个 0xFF

回复：固定为 4 个 0x55

命令说明：
在设备上按 Reset 建恢复出厂设置，设备会向服务器发送该命令，服务器接收到该命令后，需要把该设备从所有用户账号中删除。

4、L 口专用协议

4.3 0x23 设备发现 (UDP Broadcast)

User Request: |23|Dev_MAC|
Device Response: |23|IP|MAC| Key-Len | Key |
参数说明：

Dev_MAC：设备 MAC 地址，如果为 FF:FF:FF:FF:FF:FF，则所有未锁定的设备均会回复回包，如果设备已经锁定，则 Dev_MAC 必须与设备的 MAC 地址相同，则相应的设备才会回复。

IP：4 - Byte，设备局域网的 MAC 地址

MAC：6- Byte，设备 MAC 地址

Key-Len：1 - Byte，通信密钥的长度

Key：X - Byte，通信密钥

命令说明：

搜索设备命令，采用广播包形式，默认密钥加密，设备如果未锁定，则向 APP 端发送回包，回包内容包括 IP 地址、MAC 地址，加密密钥长度及 key，后面的通信采用该协商密码进行通信。

4.4 0x24 锁定设备 (UDP)

User Request: |24|dev_MAC|

Device Response: |24|Result|

参数说明：

Dev_MAC：设备 MAC 地址

命令说明：

锁定命令，锁定设备为点对点单控制，锁定模块之后模块不会响应 MAC 地址 FF:FF:FF:FF:FF:FF 的设备发现命令。

锁定设备时，请将 Flag 中的 Bit2 置 1。

5、T 口、L 口、U 口公共协议

5.1 0x61 心跳包(T: TCP | L: UDP | U: TCP)

T 口：

Request: | 61 |

Response: | 61 | Interval | Current_time |

U 口：

Request: | 61 |

Response: | 61 | Interval |

L 口：

Request: | 61 | Current_time|

Response: | 61 | Interval |

参数说明：

Current_time: 4 - Byte，当前手机的时间（UTC 时间，从 1970 年 1 月 1 日起，以秒为单位）。

Interval：2 - Byte，心跳包下次发送的间隔时间，单位秒(s)，最长时间最大为 60s

命令说明：

T 口:当 Wifi 模块请求接入成功后,向 Server 发送心跳包,Server 收到后回 复模块,模块根据返回的间隔时间发送下次心跳,从而使 Server 可以自主进行负 载调节。如果在 1.5*Interval 的时间段内，Server 没有收到模块的任何数据，则会断开该 TCP 连接。设备无法从 NTP 服务器获取时间时，可以用 Current_time 来校准时间。

U 口:由 APP 发送到 Server,由 Server 进行 Interval 控制。如果在 1.5*Interval 的时间段内，Server 没有收到 APP 的任何数据，则会断开该 TCP 连接。

L 口:由 APP 发往 Device。如果在 1.5*Interval 的时间段内,Device 没有收到 APP 的心跳数据，则会清除该 APP 的通信密钥，APP 需要重新发现设备,获取新的密钥。设备无法从 NTP 服务器获取时间时，可以用 Current_time 来校准时间。

5.2 0x62 查询模块信息(T: TCP | L: UDP | U: TCP)

Request: | 62 |

Response: | 62 | H-Len | H-Ver | S-Len | S-Ver | N-Len | Name |

参数说明：

H-Len：1 - Byte，硬件版本号长度

H-Ver：X - Byte，硬件版本号

S-Len：1 - Byte，软件版本号长度

S-Ver：X - Byte，软件版本号

N-Len：1 - Byte，设备别名长度

Name：X - Byte，设备别名

其中，软件版本号，是形如 X.Y 这样的字符串，可以解析成数值，以便检查是否有新的固件程序（参见 6.6 节 0x86 获取固件最新版本号）

5.3 0x63 设置模块别名(T: TCP | L: UDP | U: TCP)

Request: | 63 | N-Len | Name |

Response: | 63 | Result |

参数说明：

见“0x62 查询模块信息”参数说明

5.5 0x65 模块固件升级(T: TCP | L: UDP | U: TCP)

Request: | 65 | URL-Len | URL |

Response: | 65 | Result |

参数说明：

URL-Len：1 - Byte，新固件 URL 地址的长度

URL：X - Byte，新固件的 URL 地址

命令说明：

模块收到此 URL 后，会向此地址请求升级文件，完成升级工作。

6、U 口专用协议

6.1 0x81 获取工作服务器(TCP)

User Request: | 81 |

Server Response: | 81 | IP Address | Port |

参数说明：

IP Address（4 - Byte）和端口号（2 - Byte）用于服务器分布式部署时的 APP 访问重定向、负载均衡等。

命令说明：

该命令是 APP 与负载均衡服务器进行通信。APP 与某一工作服务器建立 TCP 连接之前，均需要发送该命令，获取工作服务器的 IP 和端口。

负载均衡服务器的 IP 和端口，请参照具体项目的《内层控制协议》中的定义。

该命令与特定的 WiFi 设备无关。因此，发送该命令时，帧头中的 Mac 地址，请使用智能手机的 Mac 地址。帧头中的设备类型、授权码，请使用 APP 的设备类型、授权码，请参照具体项目的《内层控制协议》中的定义。

发送该命令时，如果加密，请使用默认的密钥。

6.2 0x82 请求接入(TCP)

User Request: | 82 | ULen | UserName | PLen | Password |

Server Response: | 82 | Key Len | Key |

参数说明：

ULen : 1 - Byte ， APP 提交的登陆用户名长度

UserName : X - Byte ， APP 提交的登陆用户名

PLen : 1 - Byte ， APP 提交的登陆密码长度

Password : X - Byte ， APP 提交的登陆密码，使用 MD5 加密

Key Len：1 - Byte，密钥长度

Key：用于对之后的协议进行加密所用的密钥，密钥为服务器随机生成回复给 Device，目前暂定 IV 和 Key 值相同

命令说明：

APP 与某一工作服务器建立 TCP 连接之后，首先需要发送该命令，以便获取密钥数据。如果连接断开，重新建立 TCP 连接，则需要重新发送该命令。

该命令与特定的 WiFi 设备无关。因此，发送该命令时，帧头中的 Mac 地址，请使用智能手机的 Mac 地址。帧头中的设备类型、授权码，请使用 APP 的设备类型、授权码，请参照具体项目的《内层控制协议》中的定义。

发送该命令时，如果加密，请使用默认的密钥。

6.3 0x83 订阅/取消订阅设备事件(TCP)

User Request: | 83 | Subs_or_not | Cmd | Param |

Server Response: | 83 | Result |

参数说明：

Subs_or_not：1 字节，0x01 表示订阅，0x00 表示取消订阅。

Cmd：1 字节，事件命令的值，请查看具体项目的《内层控制协议》

Param：事件命令的参数，请查看具体项目的《内层控制协议》

命令说明：

设备的一些数据，如果发生了变化，会把该事件上报给 Server，Server 再推送给订阅了该事件的 APP。

该命令与特定的 WiFi 设备相关。因此，发送该命令时，帧头中的 Mac 地址，应该使用相对应 WiFi 设备的 Mac 地址。帧头中的厂家代码、设备类型、授权码，应该使用从设备获取到的信息。

6.4 0x84 查询设备在线/离线状态

User Request: | 84 |

Server Response: | 84 | Result |

参数说明：

Result：1 字节，0x01 表示在线，0x00 表示离线。

命令说明：

该命令与特定的 WiFi 设备相关。因此，发送该命令时，帧头中的 Mac 地址，应该使用相对应 WiFi 设备的 Mac 地址。帧头中的厂家代码、设备类型、授权码，应该使用从设备获取到的信息。

6.5 0x85 设备上线/离线事件

Server Request: | 85 | Reserved | Status |

User Response: 无

参数说明：

Reserved：1 字节，保留字节，请置 0x00。

Status：1 字节，0x01 表示在线，0x00 表示离线。

命令说明：

当 WiFi 设备与 Server 建立或断开连接时，Server 会把该事件推送给订阅了该事件的 APP。

请记得首先在 APP 中订阅、取消订阅该事件。参见 6.3 节 0x83 订阅/取消订阅设备事件。其中，Cmd=0x85，Param 为 1 字节，即这里的 Reserved。

6.6 0x86 获取固件最新版本号(TCP)

User Request: | 86 |

Server Response: | 86 | S-Len | S-Ver | URL-Len | URL |

参数说明：

S-Len：1 - Byte，软件版本号长度

S-Ver：X - Byte，软件版本号

URL-Len：1-Byte，URL 长度

URL：X-Byte，固件升级的 URL 地址

命令说明：

向服务器请求某个设备的最新版本号，以便与从设备获取到的版本号相比较，从而确定是否要执行固件更新（参见 5.2 节 0x62 查询模块信息，以及 5.5 节 0x65 模块固件升级）

该命令与特定的 WiFi 设备相关。因此，发送该命令时，帧头中的 Mac 地址，应

该使用相对应 WiFi 设备的 Mac 地址。帧头中的厂家代码、设备类型、授权码，应该使用从设备获取到的信息。