卓岚联网产品 UDP 管理端口协议

嵌入式设备联网解决方案

ZL DUI 20100427.1.0

版本信息

对该文档有如下的修改：

修改记录

日期	版本	文档编号	修改内容
2010-4-27	Rev.1	ZL DUI 20100427.1.0	发布版本
2012-8-20	Rev.2		增加参数内容
2013-3-22	Rev.3		增加参数到170字节

所有权信息

目 录

1. 概述

在联网产品处于任何工作状态下，用户都可以通过联网产品的管理端口（UDP 端口 1092）来获取联网产品的当前参数或者修改参数。参数修改后联网产品将以新参数运行，从而达到控制联网产品运行的目的。

2. 实现方法

2.1. 协议

用户通过 UDP 协议，向联网产品的 1092 端口发送如图 1 所示的命令（命令内容放在 UDP 数据包的应用层）。

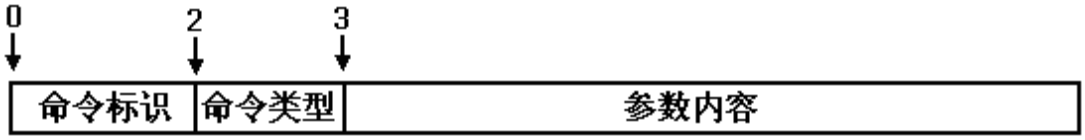

图 1 管理端口命令

其中：

命令标识：2 字节，内容必须为‘Z’和‘L’两个字符，用十六进制表示为 0x5a4c，注意是大端格式，即 0x5a 在前 0x4c 在后。

命令类型：1 字节，表示该命令的类型，如表 1 所示。

表 1 命令类型

命令名称	类 型 号	说明
PC 广播查询命令	0x00	PC 机发送该命令给联网产品，联网产品将返回设备参数给 PC。参数以设备应答命令的形式返回给 PC 机。该命令通过广播方式发送，适合于在局域网中查询所有设备。设备会以广播的方式发送“设备应答命令”给 PC 机。
设备应答命令	0x01	设备收到 PC 查询命令后，发送该命令给 PC 机，PC 机会在发送“PC 广播查询命令”的端口收到该数据。命令参数内容部分即完整设备参数。作为 TCP 客户端的设备，会每隔“保活定时时间”，向“目的 IP 或域名”的“目的端口”，以 UDP 方式发送这个命令数据包。

PC 参数修改命令	0x02	PC 机通过该命令将参数写入设备，之后设备按照新参数运行。该命令要求参数部分的 DevID（参考图 2 参数格式）必须是需要修改的设备的 DevID，用户可以从设备应答命令包中获取该设备的 DevID。PC 发送的数据包可以为单播或者广播的。 这个命令同时可以用于重启设备，如果只重启设备，不修改参数则请保持参数不变，只下发这个 0x02 命令。
PC 设置串口参数命令	0x03	PC 通过该命令修改设备串口波特率等串口参数。修改之后设备不会自动重启，也不保存参数数据。
PC 一对一查询命令	0x04	和 PC 广播查询命令的唯一区别是，PC 机不是采用广播的方式发送命令，而是向指定的 IP 发送，该命令用户通过 Internet 查询设备。设备会以非广播的方式发送“设备应答命令”给 PC 机。
IO 设置指令	0x05	参考《网络 IO 控制功能.pdf》
IO 读取指令	0x06	参考《网络 IO 控制功能.pdf》
RTS 手动模式	0x07	
RTS 自动模式	0x08	
参数通信模式	0x09	参考《向中心服务器发送模块参数功能.pdf》
参数通信模式	0x0a	保存参数的参数通信，参考《向中心服务器发送模块参数功能.pdf》

参数内容：167 字节。参数的具体格式请参考图 2 参数格式。其中“设备应答命令”、“PC 参数修改命令”中的参数内容必须是一个完整正确的参数。“PC 广播查询命令”、“PC 一对一查询命令”的参数内容，可以为任意值。“PC 设置串口参数命令”要求和串口相关的参数内容必须正确设置。

采用“PC 参数修改命令”修改参数后，设备将重启，并按照新参数运行。

注意：

1．编程时需要注意命令格式、参数格式的结构体，应该是 1 字节对齐的。

2．如果是通过 Internet 使用 UDP 管理端口协议，那么需要在设备端的路由器上将 1092 端口映射到设备所在 IP 的 1092 端口上。且使用 PC 一对一查询命令，查询设备参数。

2.2. 参数格式

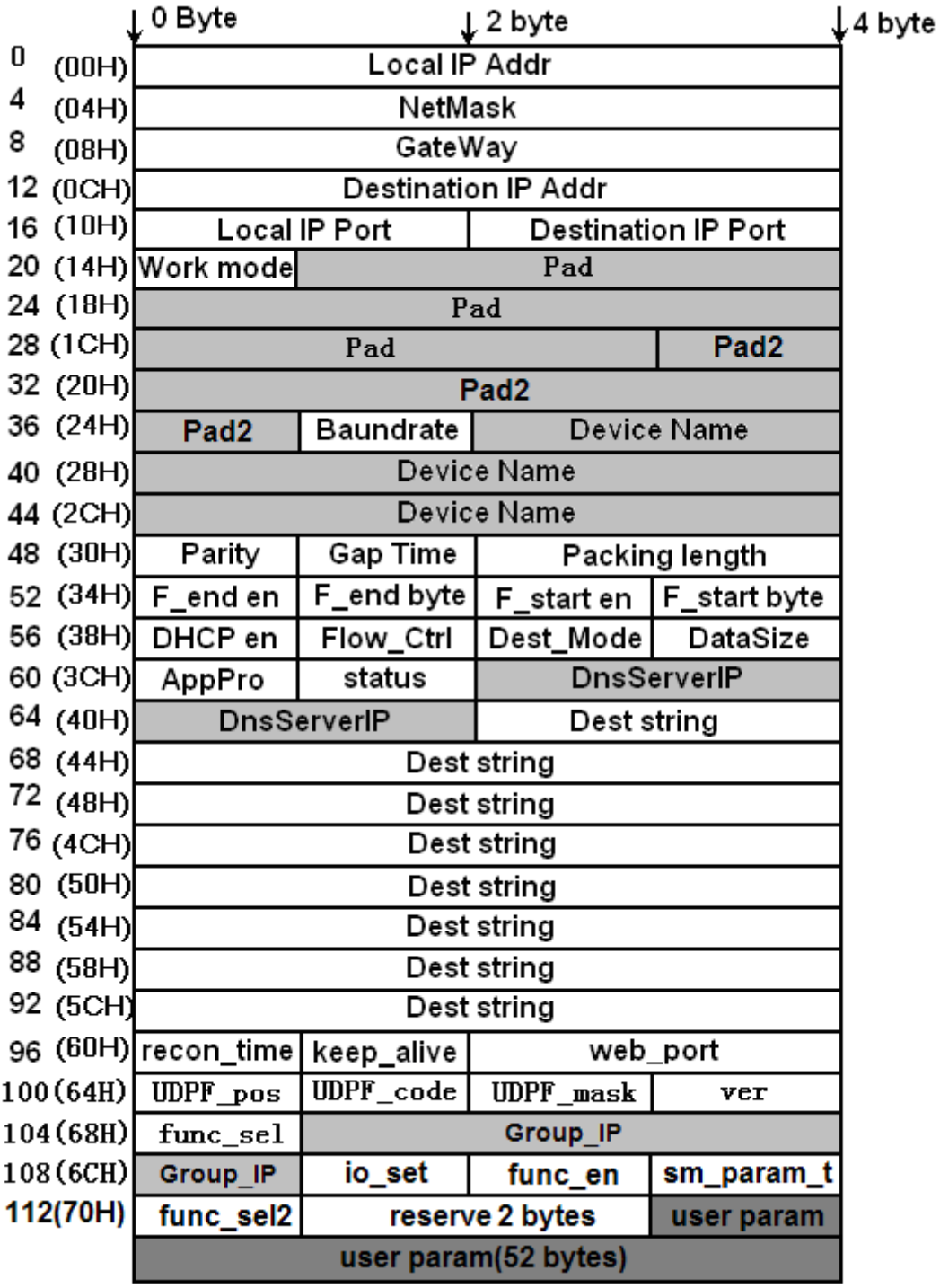

图 2 参数格式

如图 2 所示为模块参数格式，发送和接收参数时，第 1 字节先发送。上图

中的字节采用大端模式（big-endian），例如 Local IP Addr 的高字节在左边。各参数的含义请参考《ZLSN2000 数据手册》。

1. Local IP Addr（本地 IP 地址）：4 字节。
2. Net Mask(子网掩码)：4 字节。
3. GateWay（网关）：4 字节。
4. Dest IP（目的 IP）：4 字节。具有 DNS 功能的联网产品，该字段的作用被 DestString 字段代替，该字段无效；不具有 DNS 功能的联网产品，该字段使用 4 字节表示的目的 IP 地址。您的产品是否具有 DNS 功能请咨询卓岚公司。
5. Local IP Port（本地端口）：2 字节。
6. Dest Port（目的端口）：2 字节。
7. Work mode（工作模式）：1 字节。数值 0、1、2、3 分别对应：服务器模式（TCP Server）、客户端模式（TCP Client）、UDP 模式、UDP 组播模式。
8. Pad（填充区）：10 字节，应该全部为 0。
9. Pad2（填充区 2，也即 DevID）：6 字节。
10. Baundrate（波特率）：1 字节。从 0～13（13 表示 460800）分别对应：1200、2400、4800、7200、9600、14400、19200、28800、38400、57600、76800、115200、230400、460800。
11. Device Name（设备名称）：10 字节。必须是以 0 结尾的可见字符串。
12. Parity（奇偶位）：1 字节。0～4 分别对应：None、Even、Odd、Mark、Space 五种方式。
13. Gap Time（间隔时间）：1 字节。
14. Packing length （包长度）：2 字节，数值范围 1～1400。
15. F_end en（帧尾字符有效位）：1 字节，0、1 分别表示帧尾规则不起作用、起作用。V1.472 版本开始这个字节不再有效。
16. F_end byte（帧尾字符）：1 字节。V1.472 版本开始这个字节不再有效。
17. F_start en（帧首字符有效位）：1 字节，0、1 分别表示帧首规则不起作用、起作用。V1.472 版本开始这个字节不再有效。
18. F_start byte（帧首字符）：1 字节。V1.472 版本开始这个字节不再有效。
19. DHCP en（DHCP 有效位）：1 字节。0、1 分别表示使用静态 IP、使用 DHCP 获得 IP。
20. Flow Control（流控方式）：1 表示采用 CTS、RTS 流控；0 表示不采用流控。

21. Dest_Mode(目的模式)：1 字节。0、1 分别表示静态模式和动态模式。
22. DataSize（串口位数）：8～5bit，分别对应 0、1、2、3。
23. AppPro（转化协议）：0 表示透明传输，1 表示 Modbus TCP 和 Modbus RTU 之间的转化，2 表示 RealCom。
24. Status（修改模式）：读取该参数时，Status 的 bit0=1 表示当前 TCP 连接已建立或者处于 UDP 状态，否则 bit0=0。这个字段提供了读取联网模块当前状态的一个方法。
25. DnsServerIP（DNS 服务器 IP）：设置为 DNS 服务器 IP，4 字节。
26. Dest string（目的地址）：具有 DNS 的联网产品，该字段表示目的 IP 字符串，例如写入“192.168.0.3”这个字符串为十六进制：0x31, 0x39, 0x32, 0x2e, 0x31, 0x36, 0x38, 0x2e, 0x30, 0x2e, 0x33, 0x00。注意最后添加一个字符串末尾 0。不具有 DNS 功能的联网产品该字段无效。
27. Recon_Time（断线重连时间）：1 字节，范围 0～255。
28. Keep_Alive（保活定时时间）：1 字节，范围 0～255。
29. Web_port(网页访问端口)：2 字节，通过浏览器访问网页的端口。
30. UDPF_pos、UDPF_code、UDP_mask（UDP 应用层滤波参数）：共 3 个字节，一般都设置为 0，即可。该参数目前已经无效。
31. ver（模块版本）：1 个字节，不可修改。ver=0 是表示版本号为 1.383。实际的版本号为 383+ver，例如 ver=117，表示版本为 1.500。
32. func_sel（模块支持的功能）：1 个字节，无法修改。每位的具体含义如下：bit0=1 表示支持网页下载；bit1=1 表示支持 DNS 域名系统；bit2=1 表示支持 REAL_COM 协议；bit3=1 表示支持 Modbus TCP 转 RTU；bit4=1 表示支持串口修改参数；bit5=1 表示支持自动获取 IP（DHCP）；bit6=1 表示支持存储扩展 EX 功能；bit7=1 表示支持多 TCP 连接。
33. Group_IP（UDP 组播地址）：4 个字节，范围 224.0.0.0 到 239.255.255.255。
34. io_set（IO 端口设置）：IO 端口控制字，请参考 IO 控制相关文档。
35. func_en（功能选择）：功能选择/使能控制字。bit0=1 打开“数据重启功能”，bit1=1 打开“向中心服务器发送模块参数功能”。bit2=1 打开“修改参数需密码功能。bit3=1 打开“UDP 进制接收广播包功能”。请参考相关文档那个。
36. sm_param_t（sm 参数时间）：向中心服务器发送模块参数功能发送间隔时间，单位为分钟。

37. func_sel2（模块支持的功能 2）：该模块支持的高级功能。bit0=1 表示支持 IO 配置功能。bit1=1 表示支持 UDP 组播功能。bit2=1 表示支持多目标 IP 功能。
38. 保留 54 字节。该保留的 54 字节留作将来升级使用。参数总字节数为 167 字节（对于 UDP 管理端口协议，需加上头部 2 个标识和 1 个命令类型，总长度为 170 字节）。

参数格式的 C 描述为：

```
typedef unsigned char    zl_u8;
typedef char             zl_s8;
typedef unsigned short   zl_u16;
typedef short            zl_s16;
typedef unsigned long    zl_u32;
typedef bit              zl_bool;
typedef signed     long  zl_s32;

typedef zl_u32 IP_ADDR;

#define MAX_KEY_LEN                 10
#define MAX_DEV_NAME_LEN            10
#define ETHER_ADDR_LEN              6
#define DNS_NAME_MAX_LEN        30

struct SSServerParam
{
    IP_ADDR param_local_ip;
    IP_ADDR param_net_mask;
    IP_ADDR param_gate_way;
    IP_ADDR param_dest_ip;
    zl_u16 param_local_port;
    zl_u16 param_dest_port;
    zl_u8 param_work_mode;
    zl_s8 param_key[MAX_KEY_LEN];
    zl_u8 ether_addr[ETHER_ADDR_LEN];
    zl_u8 baundrate_index;
    zl_s8 dev_name[MAX_DEV_NAME_LEN];
    zl_u8 param_parity;
    zl_u8 param_max_no_s_data_interval;
    zl_u16 param_max_data_len;
    zl_u8 param_fram_end_en;
    zl_u8 param_frame_end_byte;
    zl_u8 param_fram_start_en;
    zl_u8 param_frame_start_byte;
    zl_u8 param_ip_mode;
    zl_u8 param_flow_control;
    zl_u8 param_dest_dynamic;
    zl_u8 param_data_bits;
    zl_u8 app_protocol;
```

```
        zl_u8 status;
        IP_ADDR dns_server_ip;
        zl_s8 dns_name[DNS_NAME_MAX_LEN];
        zl_u8 keep_alive_time;
        zl_u8 reconnect_time;
        zl_u16 web_port;
        zl_u8 udp_filter_pos, udp_filter_code, udp_filter_mask;
        zl_u8 ver;
        zl_u8 func_sel;
        IP_ADDR udp_group_ip;
        zl_u8 io_set;
        zl_u8 func_en;
        zl_u8 server_mode_param_t;
        zl_u8 func_sel2;
        zl_u8 var1[2];
        zl_u8 var2[52];
};
```

3. 具体例子

这里通过卓岚 SocketDlgTest 来发送和接收以上的 UDP 管理数据包。

3.1. 读取参数

3.1.1. 自动搜索

自动搜索对应 zlvircom 程序的设备管理里面的“自动搜索”功能，它适用于局域网内部的搜索。

如图 3 所示，首先设置 UDP 目的 IP 为 255.255.255.255，目的端口为 1092，点击“打开”按钮。选择十六进制发送选项，在发送信息区，写入一个 PC 广播查询命令数据包：

5a 4c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00

该数据包中，5a 4c 是命令标识，00 是命令类型，后续的 167 个 0 是参数内

容，由于是查询参数内容没有关系，所以都用 0 代替。这里参数内容个数 167 可能随着版本的不同而有所不同。点击“UDP 发送”按钮，发送该数据包。此后在接收信息区收到设备的应答设备应答命令数据包：

5a 4c 01 c0 a8 01 a9 ff ff ff 00 c0 a8 01 01 c0 a8 01 39 10 64 10 64 00 38 38 38 38 38 38 38 38 38 38 5a 4c 6f 73 cc d6 04 30 30 30 30 30 30 30 30 31 00 00 03 05 14 00 00 00 00 00 00 01 00 00 01 08 08 04 04 31 39 32 2e 31 36 38 2e 31 2e 35 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 3c 00 50 00 00 00 8a b6 e6 5a 4c 01 00 00 05 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

这里，5a 4c 是命令标识，01 表示设备应答命令类型，之后是 167 个字节的设备参数。例如这里的 c0 a8 01 c8 就是 IP 地址 192.168.1.200。这里的参数数量 167 可能随着版本的不同而不同，但是都会大于 90 个字节。

如果网络中有多个设备会收到多个设备应答命令数据包。

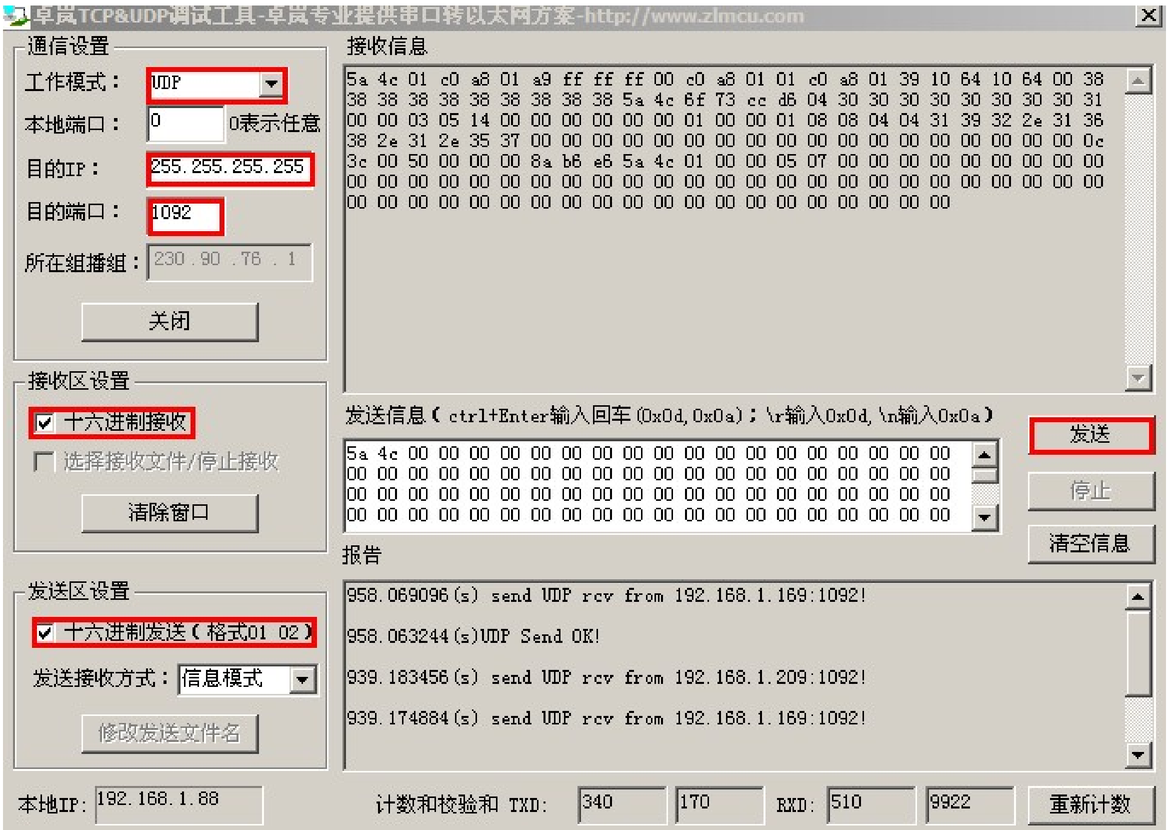

图 3 PC 广播查询命令

3.1.2. 手动添加

手动添加类似 zlvircom 程序设备管理里面的“手动添加”功能。适用于添加外网的设备。

如果采用一对一方式查询参数，那么如图 4 所示，不同点是 UDP 目的 IP 改为设备的 IP，命令类型改为 04。同样可以收到 192.168.1.200 这个设备的应答。

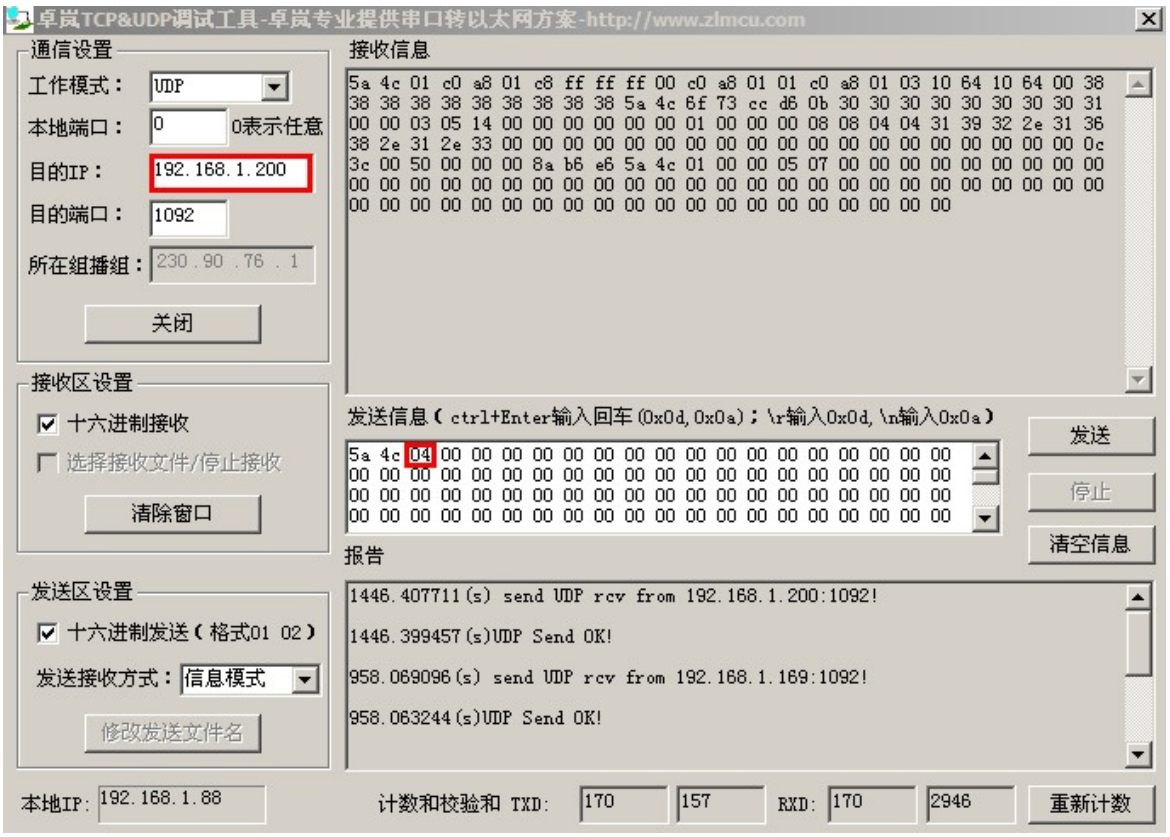

图 4 PC 一对一查询命令

3.2. 修改参数

设备首先通过读取参数的方法获得参数内容，那么现在假设用户需要修改设备的目的 IP 为 192.168.1.4。修改目的 IP 应该修改参数 DestString，从图 2 参数格式查到 DestString 的在参数中的偏移量应该为 66，在读取的参数内容中找到偏移 66 的地方（注意 66 是指参数内容，不含有开头的 3 个字节的 5a 4c 01），修改该值为 192.168.1.4，结果如下（黑体部分为修改的 IP，IP 以字符串表示）：

c0 a8 01 a9 ff ff ff 00 c0 a8 01 01 c0 a8 01 39 10 64 10 64 00 38 38 38 38 38 38

38 38 38 38 **5a 4c 6f 73 cc d6** 04 30 30 30 30 30 30 30 30 31 00 00 03 05 14 00 00 00 00 00 00 01 00 00 01 08 08 04 04 **31 39 32 2e 31 36 38 2e 31 2e 34 00** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 3c 00 50 00 00 00 8a b6 e6 5a 4c 01 00 00 05 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

注意其中的 DevID（上面的 **5a 4c 6f 73 cc d6**），应该是该设备的 DevID，如果是从读取的参数中获取的则没有问题（即将接收到的参数中的 01 命令改为 02 命令，然后将需要修改的参数修改后重新发送出去）。将以下数据，发送给 192.168.1.200 的设备：

5a 4c 02 c0 a8 01 a9 ff ff ff 00 c0 a8 01 01 c0 a8 01 39 10 64 10 64 00 38 38 38 38 38 38 38 38 38 38 5a 4c 6f 73 cc d6 04 30 30 30 30 30 30 30 30 31 00 00 03 05 14 00 00 00 00 00 00 01 00 00 01 08 08 04 04 31 39 32 2e 31 36 38 2e 31 2e 34 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 3c 00 50 00 00 00 8a b6 e6 5a 4c 01 00 00 05 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

如图 5 所示。之后可以用设备管理软件（ZLVircom）看到设备的目的 IP 已经修改。

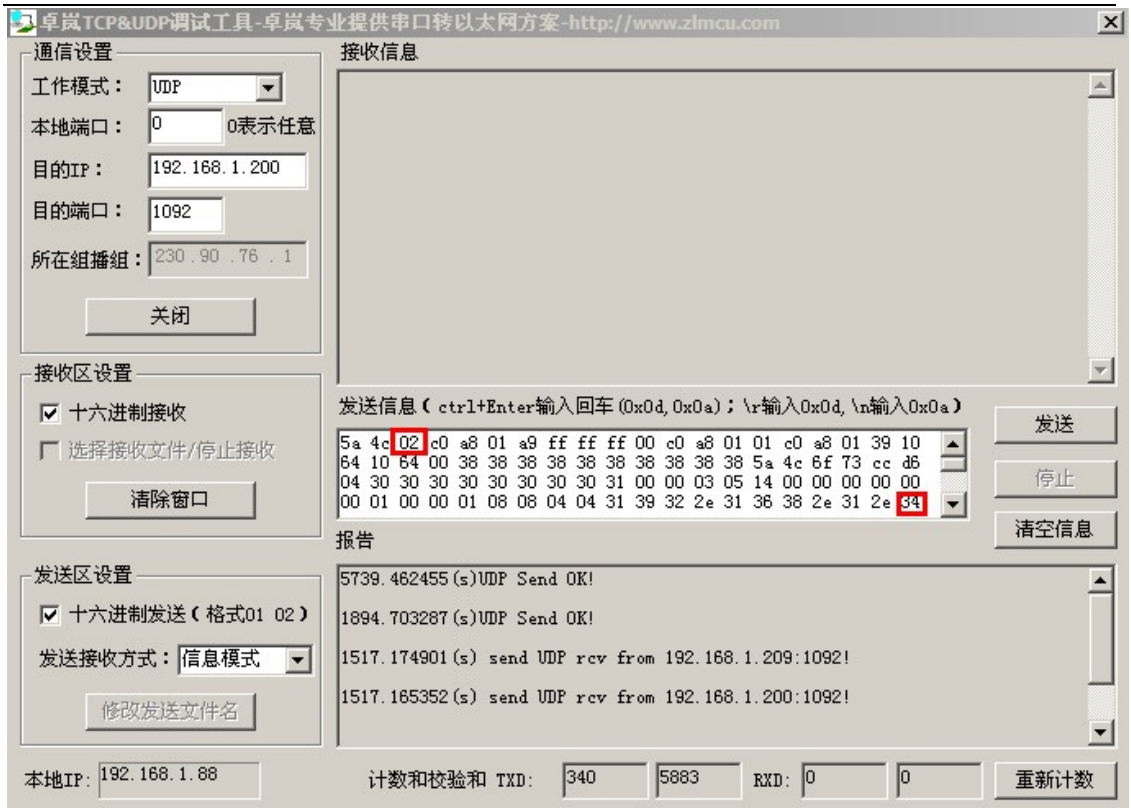

图 5 修改参数命令

PC 设置串口参数命令的例子同修改参数参数命令类似，只不过将命令类型从 02 变为 03。

3.3. 获得模块连接状态

在图 2 参数格式中有一个参数是 status（61 位置），这个变量为 0 则表示模块认为 tcp 连接没有建立，否则表示 tcp 连接已经建立。

3.4. 外网模块修改

由于，对于外网作为 TCP 客户端的设备，会每隔“保活定时时间”，向“目的 IP 或域名”的“目的端口”，以 UDP 方式发送这个命令数据包，那么如果 PC 机在这个端口接收 UDP 参数数据包，就可以查询到这个设备的状态。对于跨网关的来自外网的 TCP 客户端的模块，如果需要修改其参数，那么请使用 PC 参数修改命令 0x02，写设备的目的端口就不是 1092 了，而是设备的来路的源 IP 和源端口。其它和局域网内的修改一样。

3.5. 重启固定 IP 的设备

如果需要重启一个固定 IP 的设备。那么首先根据 3.1.1 自动搜索一节介绍的向这个 IP 的 1092 端口发送 04 命令的数据包。然后设备会回复一个长度相同的数据包。然后 PC 再将这个回复的数据包的命令控制字改为 02 命令，回复给设备，这样设备收到后就会重启。

3.6. 利用定时发送参数

卓岚模块具备“定时发送参数功能”，具体参考《向中心服务器发送模块参数功能》。简单的说，就是勾选定时发送参数，然后设备会定时向目的 IP 或者域名发送“UDP 管理协议的 0x01 命令”（见表 1 命令类型），服务器（这里是 192.168.1.188）会每隔 5 分钟收到这个 01 命令。这就为服务器设置设备、重启设备提供了途径。

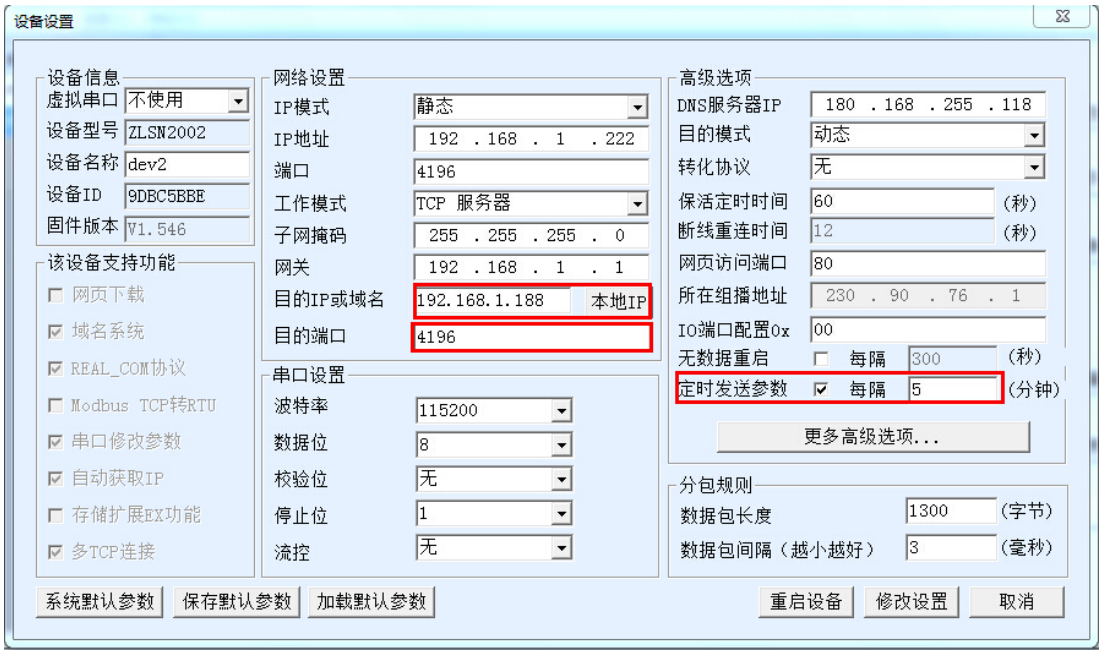

图 6 定时发送参数

需要控制设备的时候，可以通过服务器反馈一个 0x02 修改参数命令来实现，因为设备收到任何 0x02 命令都会重启。为了防止随意修改参数，最简单的做法是，当服务器收到 0x01 命令后尽快将命令类型（第 3 个字节）从 0x01 修改为 0x02，返回给设备。对这个操作做如下说明：

1. 最好检查收到的指令是 0x01 指令，再做返回 0x02。如果设备发过来的是 0x09 和 0x0a 指令，可能参数不对。

2. 返回是指，向这个 UDP 包的来路 IP 和来路端口发送。发送时只要将来路的数据包的第三个字节修改为 0x02 即可。
3. 返回时间：注意请在收到设备 0x01 命令的 1 分钟内返回，否则可能数据会无法到达设备。
4. 判断设备：通过收到的 0x01 命令中的参数区的 ID 可以判断是哪个设备过来的，借助于这个 ID 也就能够实现对特定的设备进行重启的功能。

3.7. 注意事项

1. 搜索设备代码编写注意事项：
   a) 发送和接收用的 socket 套接字 fd 应该为非阻塞的，这样在后面调用 recvfrom()接收设备的应答 UDP 包时就不会阻塞，方便多次调用。
   b) 在局域网内搜索设备时，发送完“PC 广播查询命令”后应该等待至少 100ms，再用套接字 fd 进行接收，立即接收是接收不到应答 UDP 包的。
   c) 使用套接字 fd 接收时，应该多次反复接收，以接收局域网中的所有的设备的应答。如果只接收一次则只能找到第一个应答的设备。
   d) 应该丢弃图 1 中命令标识和命令类型不对的 UDP 数据包。
   e) 参数中的 DevID 是不会变的，而且每个产品都不同，可以做为设备的标识。（DevID 的位置参考图 2 参数格式）。

4. 动态连接库

卓岚提供 ZLDevManage.dll 动态库，实现以上的网络协议。用户只要调用接口即可。具体参考《卓岚设备管理函数库用户手册》

5. 售后服务和技术支持

上海卓岚信息技术有限公司
地址：上海市徐汇区漕宝路 80 号光大会展 D 幢 12 层
电话：021-64325189
传真：021-64325200
网址：http://www.zlmcu.com
邮箱：support@zlmcu.com