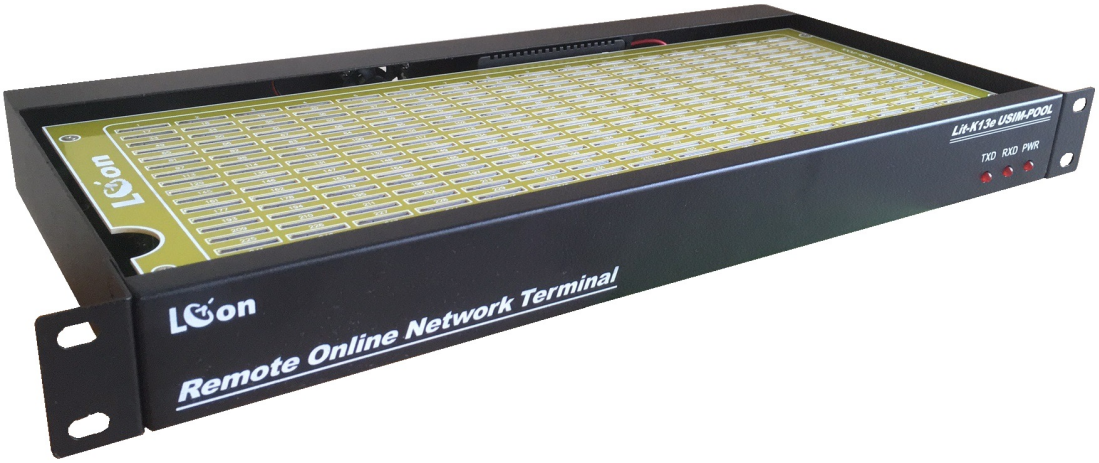
网络在线卡池
Lit-K13e-V60



使用说明书

目录

深圳市鑫狮通讯设备开发有限公司.
地址：深圳市罗湖区经二路38号　清园A602
电话： 0755-82224022
网站：http://www.xin-lion.com
技术支持QQ：1985768303

第一章：产品型号说明

本公司所有系列产品，依据下列规则划分型号

根据以上规则，因此本产品为以太网接口的256路SIM卡远程在线卡池

第二章：产品介绍

1、 应用领域

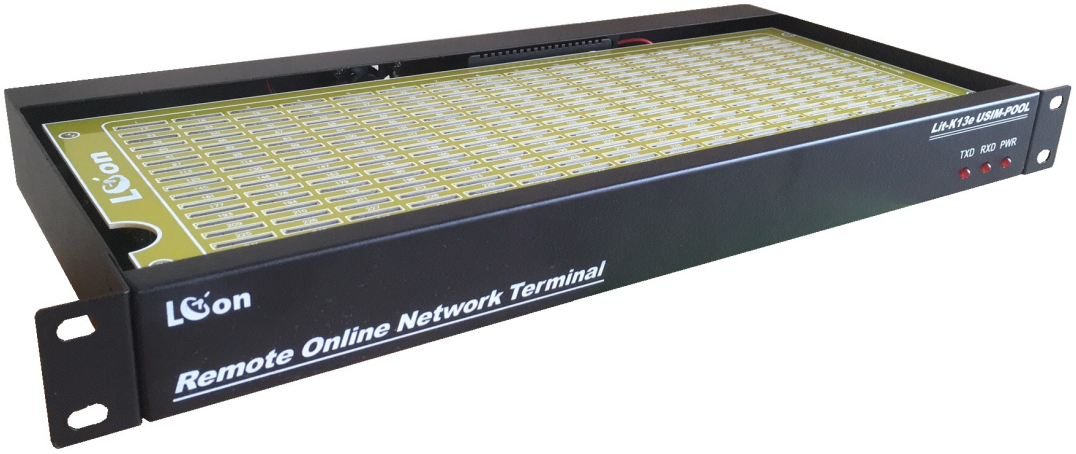
随着各大移动运营商宽带网络的不断升级，原来的2G、3G网络逐步升级为4G,甚至以后还可能升级为5G网络，移动互联网产业无疑将成为接下来一段时间最强劲的经济增长点和技术革命方向。

但是由于产业垄断(尤其在中国)，移动上网用户支付的流量费用也将是用户最心疼的开支之一。大量的流量套餐限制让很多用户使用起来小心翼翼，惊恐万分。

有些国家或省份的运营商发行的当地流量卡在价格上还是很有吸引力的，但是我们在旅游的时候不可能每到一个地方就买一张当地的手机卡，离开之后就丢弃。于是一种手机与卡分离，自动远程配置最合适的手机卡给客户使用的运营系统出现了。本产品就是这个系统中最重要的一环所用到的设备，每个设备管理256张SIM卡，安装在在机房的固定机架上，由服务器统一管理。

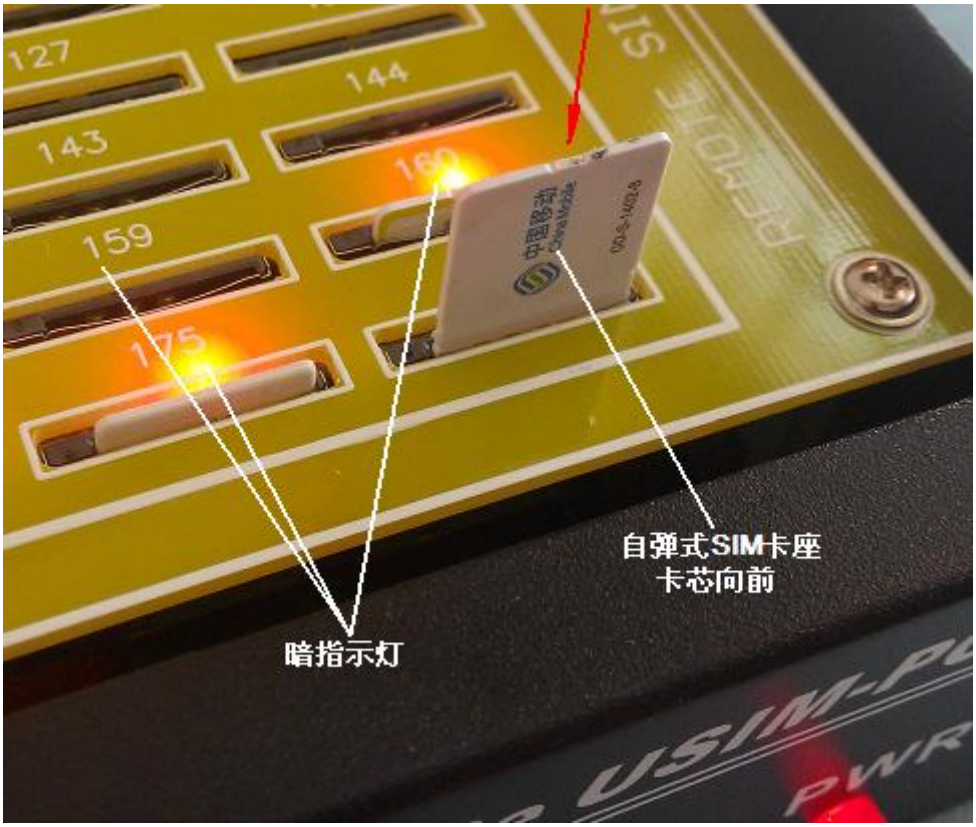
当然不仅仅是旅游，在其他的方面，比如说车联网也同样需要节省漫游费用，因此应用领域较为广阔，如下图

2、 产品外型



正面(标准1U机箱结构)

背面接口定义(440 x 220 x 44 单位:mm)



SIM卡安装

第三章：产品特点

1、 基本功能

Lit-K13e网络在线卡池可以实现1-256张SIM卡的管理，提供这些卡同时在线给远程手机使用。每张卡的实际操作命令只有三个，那就是启动、停止和通讯。通讯时透明传输远端手机与SIM卡之间的数据，严格遵守ISO-7816智能卡管理规范和GSM11.11通讯管理规约.

每张手机卡都有一个专用指示灯，未插卡时灯灭，插上卡未启动为常亮，快闪(每秒亮三下)为工作状态，慢闪(2.47秒灭，0.03秒亮)为SIM卡异常.

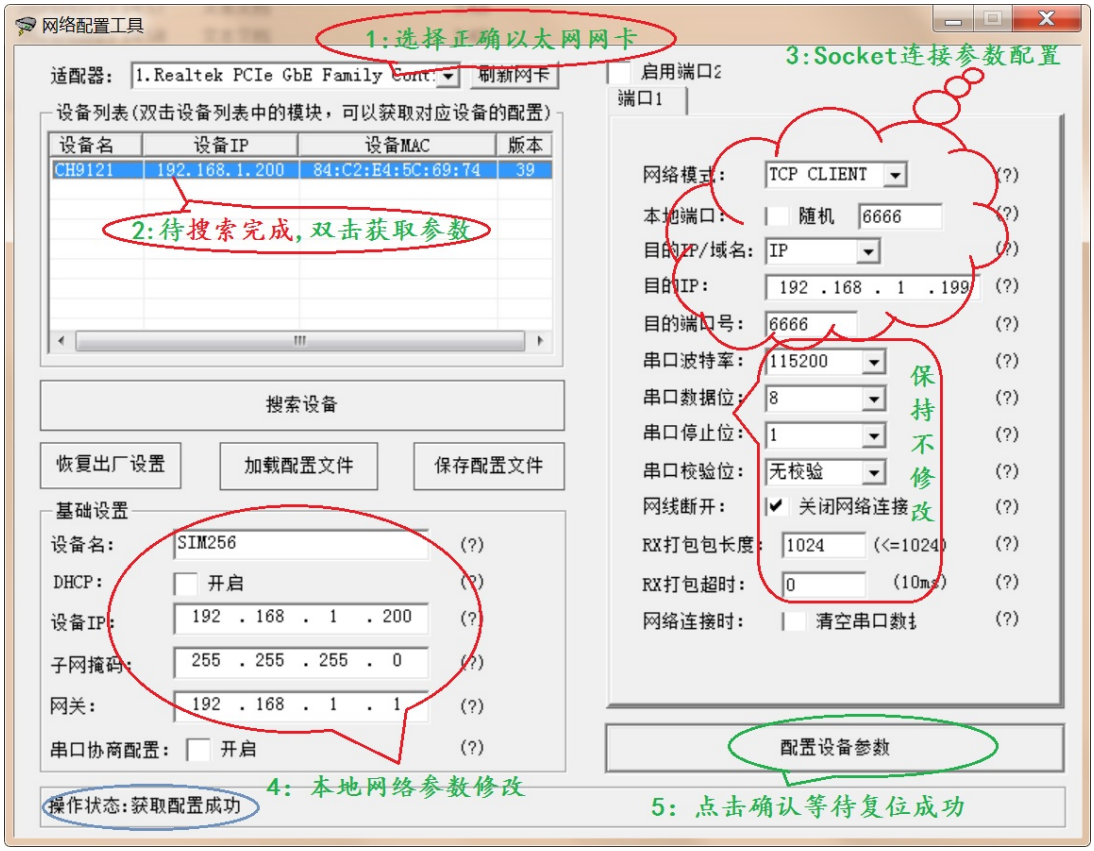
整机的SIM卡状态，及版本和ID号也可以通过端口读出，

详见“通讯协议”部分

2、 技术参数

- 出厂默认为 192.168.1.199 TCP服务端口为 6666
- 电源使用AC220V, 功耗 <12W
- 重量2.7kg
- 标准1U机箱设计 体积：440 x 220 x 44 单位:mm

3、 网络参数设置



- 在同一个局域网内，打开网络配置工具NetModuleConfig.exe，如上图
- 选择正确的网卡，点击搜索设备，注意操作状态提示，按照图上的提示步骤操作
- 串口参数部分不要修改，保持115200bps,N,8,1

第四章：通讯协议

1、 协议规则

- 本协议适用于鑫狮通讯所研发的以太网接口在线SIM卡池
- 协议中涉及到的所有数据都是16 制表达方式,如果是ASCII码所反映的具体字符会用绿色括号加以辅助说明，例如数据: 30 31 39 (019)
- 所有协议都是一问一答方式，即上位机询问，下位机回答。根据网络状态和协议内容不同，回答时间有快有慢，下位机回答时间在1-1000mS之内。超过1000mS没有数据返回，说明回答完毕或通讯中断。
- 问答不是一对一等待回答方式。就是说可发同时并发多个不同SIM卡命令，哪个先回答哪个就先返回。

2、 协议格式

1 上位机下发数据包格式

报头 (2Byte)	卡号 (1Byte)	长度 (1Byte)	数据 (nByte)

- ***报头：*** **AA 66** 两个固定字节
- ***卡号：*** 一个字节：如果是**00-FF(1-256**卡)表示对具体的SIM卡操作。
- ***长度：*** 表示此条命令后面数据部分的字节长度,1字 。
  此处长度为1表示 指定SIM卡的操作或整机操作。
  根据ISO-7816 命令数据不可能小于2,因此长度≥2时，为对该SIM卡的通讯命令
- ***数据：*** 根据前面部分的介绍数据部分定义如下表。

报头	卡号	长度	数据	命令解释	返回
AA66	00-FF	01	FF	*启动SIM卡*	返回ATR
			00	*停用SIM卡*	无返回
			01	*查看卡池ID号*	返回12字节的卡池ID号#
			02	*查看卡池版本号*	返回4字节的卡池版本号#
			03	*查看256个SIM卡的状态*	返回256字节SIM卡状态*#
			04	*向SIM卡发送错误指示*	无返回
		02-FF	内容	*发送通讯命令*	返回命令结果

* 返回256字 按照 序分 代表1-256号卡，**00**:表示未插卡 **55**:表示插卡未启

动 **AA**:表示插卡工作中 **FF**:表示异常
对整机设备操作，卡号为任意数值，返回时卡号为**00**

2 卡池返回数据包格式

报头 (2Byte)	卡号 (1Byte)	长度 (2Byte)	数据 (nByte)

- ***报头：*** 正确返回**AA 55**(对SIM卡操作)或**AA 44**(对设备操作)两个字节
- ***卡号：***一个字节：如果是**00-FF**表示具体的SIM卡返回数据
  对整机设备操作的命令，返回时卡号为**00**
- ***长度：*** 两个字节(*此处注意，与下发命令不同*),高位在前，低位在后，仅仅表示数据部分的字节个数.
- ***数据：***该条协议所携带的具体数据，没有数据时为空

3、 协议举例

- 查询设备ID码（12字节HEX数据）

--> AA 66 00 01 01

- **<-- AA 44 00 00 0C FF 75 06 71 82 55 54 33 39 20 67 00**

- 查询设备版本号 （“V057”）

--> AA 66 00 01 02

<-- AA 44 00 00 04 56 30 35 37

- 查询设备所有SIM卡工作状态

--> AA 66 00 01 03

<-- AA 44 00 01 00 AA 55 00 FF 11.....55

(1卡*工作中*， 2卡、256卡*未启动*，3*卡未插*，4*卡异常*，5*卡未知状态*(只有这5种状态))

- 告诉设备第38卡异常

--> AA 66 25 01 04

<-- 无

◆ 启动第101张SIM卡 (返回ATR)

--> AA 66 64 01 FF

<-- AA 55 64 00 11 3B 3D 94 00 32 06 01 12 00 00 86 60 61 10 80 00 07

◆ 停用第100张SIM卡

--> AA 66 63 01 00

<-- 无

◆ 向第102张SIM卡发命令 A0 A4 00 00 02

--> AA 66 65 05 A0 A4 00 00 02

<-- AA 55 65 00 01 A4

第五章：终端开发相关知识(ISO-7816)

1．手机及SIM卡开机工作原理

正确使用此产品，需要对SIM卡工作原理有所了解。

众所周知，每个手机都有个SIM卡，SIM卡是一个符合ISO-7816国准的智能卡。手机在开机工作时会向SIM卡加载电压，然后向SIM卡的RESET脚发送复位脉冲，在脉冲发送完毕后，SIM卡会返回ATR信息。根据ATR的信息，我们可以判断出SIM卡的基本信息。

此后SIM卡与手机与基站之间进行了一系列的数据交换，才能得到鉴权中心的认可，允许用户使用各项约定好的业务。但是一般的情况下我们的SIM卡与手机是本地连接的，直接向SIM卡座的IO口读写数据即可。现在我们要使用卡池中的SIM卡，自然手机开机后就不能再向本地SIM卡座读取信息了。而是更改启动程序，使得手机开机或者复位后，先与卡池(或者与服务器再通过服务器与卡池)之间建立数据连接通道。这个通道的建立一般是通过wifi连接或者类似于双卡手机先激活其中一张SIM卡进行网络连接。然后向自己想要的SIM卡发送启动命令，得到ATR。此后的过程与本地SIM卡操作没有区别，唯一不同的就是因为是网络通讯，延时可能稍微要长，因此SIM卡池安放在尽可能快速的网络环境中。

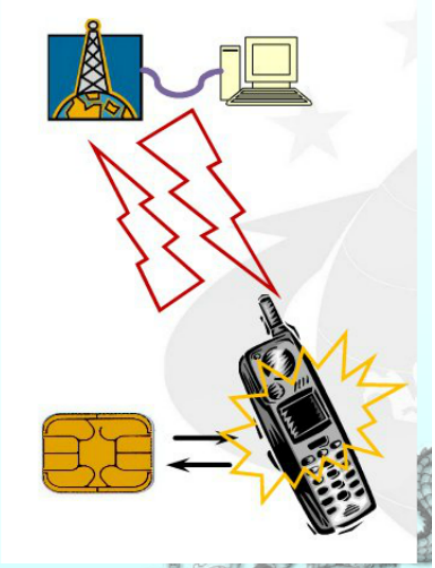
另外卡池在转发命令的时候是透明传输的，不对过程中数据进行解码。因此任何更改SIM卡通讯波特率(ETU)的指令不要进行操作，否则会造成之后的通讯失败。

2．SIM卡登陆基站进行鉴权的过程

SIM卡用户身份鉴权：确认用户身份是否合法，鉴权过程是在是在网络和SIM卡之间进行的，而鉴权时间一般是在移动终端登记入网和呼叫时。鉴权开始时，网络产生一个128比特的随机数RAND，经无线电控制信道传送到移动台，
SIM卡依据卡中的密钥Ki和算法A3,对接收到的RAND计算出应答信号SRES，并将结果发回网络端。而网络端在鉴权中心查明该用户的密钥Ki，
用同样的RAND和算法A3算出SRES,并与收到的SRES进行比较，如一致，鉴权通过。

入网鉴权过程

1. 开机；
2. 手机从卡片上读取IMSI；
3. 手机将IMSI发送给服务器；
4. 服务器生成一组随机数，并发送回手机；
5. 手机将随机数发送给SIM卡；
6. SIM卡根据随机数和Ki算出结果（SRES），并传送给手机；
7. 手机将SRES传给服务器；
8. 服务器从数据库中找到与此IMSI对应的Ki，并使用相同随机数、相同算法计算出SRES'，并比较；
9. SRES=SRES'=>鉴权成功！ 否则鉴权失败



注：
IMSI：国际移动客户识别码，用于匹配手机号，共16位
Ki：用户鉴权秘钥，即客户身份认证密码，存放在特定区域，不能读取，共32位

第六章：辅助开发示例

1. 用卡池发协议读第17个SIM卡ICCID号过程

==>**AA661101FF** (启动第18个SIM卡)
<==AA 55 11 00 16 3B 9F 95 80 1F C3 80 31 E0 73 FE 21 13 57 86 81 02 86 98 44 18 A8

==>**AA661105A0A4000002**
<==AA 55 11 00 01 A4

==>**AA6611023F 00**
<==AA 55 11 00 02 9F 17

==>**AA661105A0A4000002**
<==AA 55 11 00 01 A4

==>**AA6611022FE2**
<==AA 55 11 00 02 9F 0F

==>**AA661105A0B000000A**
<==AA 55 11 00 0D B0 98 68 00 34 91 41 28 91 60 63 90 00
(第17个SIM卡的ICCID: 89 86 00 43 19 14 82 19 06 36)

2. 用卡池发协议读第256个SIM卡IMSI号过程

==>**AA66FF01FF** (启动第256个SIM卡)

<==AA 55 FF 00 15 3B 9E 94 80 1F 47 80 31 A0 73 BE 21 11 66 44 4D 54 22 01 00 26

==>**AA66FF05A0A4000002**

<==AA 55 FF 00 01 A4

==> **AA66FF027F20**

<==AA 55 FF 00 02 9F 17

==>**AA66FF05A0C0000017**

<==AA 55 FF 00 1A C0 00 00 00 00 7F 20 02 00 00 00 00 00 0A 93 00 30 04 00 83 8A 83 8A 00 90 00

==>**AA66FF05A0A4000002**

<==AA 55 FF 00 01 A4

==>**AA66FF026F07**

<==AA 55 FF 00 02 9F 0F

==>**AA66FF05A0B0000009**

<==AA 55 FF 00 0C B0 08 49 06 10 89 49 10 63 51 90 00

(第256个SIM卡的IMSI: 08 49 06 10 89 49 10 63 51)

3. 用卡池发协议发送第2个SIM卡的GSM鉴权过程

==>**AA660101FF** (启动第256个SIM卡)

<==AA 55 01 00 14 3B 9D 95 80 1F C7 80 31 E0 73 FE 21 13 65 15 09 63 86 83 A1

==>**AA660105A0A4000002**

<==AA 55 01 00 01 A4

==> **AA6601023F00**

<==AA 55 B0 00 02 9F 17

==>**AA660105A0A4000002**

<==AA 55 01 00 01 A4

==> **AA6601027F20**

<==AA 55 B0 00 02 9F 17

==>**AA660105A088000010**

<==AA 55 01 00 01 88

==>**AA66011012305263415263524195637485967463** (送随机数)

<==AA 55 01 00 02 9F 0C

==>**AA660105A0C000000C**

<==AA 55 01 00 0F C0 50 89 06 FE 24 EC FE 3A 22 90 BD 8C 90 00

(第2个SIM的 GSM鉴权结果,3G使用双向鉴权，激活过程较复杂，这里不再举例)