InDTU932 南网加密模块

快速入门指南

资料版本：V1.0—2019.11

www.inhand.com.cn

北京映翰通网络技术股份有限公司

声明

首先非常感谢您选择本公司产品！在使用前，请您仔细阅读本用户手册。

非本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

由于不断更新，本公司不能承诺该资料与实际产品一致， 同时也不承担由于实际技术参数与本资料不符所导致的任何争议，任何改动恕不提前通知。本公司保留最终更改权和解释权。

本手册图形界面约定

格 式	意 义
	表示按钮名，如“单击确定按钮”。
“”	表示窗口名、菜单名，如：弹出“新建用户”窗口。
>>	多级菜单用“>>”隔开。如“文件>>新建>>文件夹”多级菜单表示“文件”菜单下的“新建”子菜单下的“文件夹”菜单项。
注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
说明	对操作内容的描述进行必要的补充和说明。

技术支持联络信息

北京映翰通网络技术股份有限公司（总部）

电话：010-84170010

地址：北京市朝阳区紫月路18号院3号楼5层

成都办事处

电话：028-8679 8244

地址：四川省成都市高新区府城大道西段399号，天府新谷10栋1406室

广州办事处

电话：020-8562 9571

地址：广州市天河区棠东东路5号远洋新三板创意园B-130单元

武汉办事处

电话：027-87163566

地址：湖北省武汉市洪山区珞瑜东路 2 号巴黎豪庭 11 栋 2001 室

上海办事处

电话： 021-5480 8501

地址：上海市普陀区顺义路18号1103室

目 录

1 连接设备

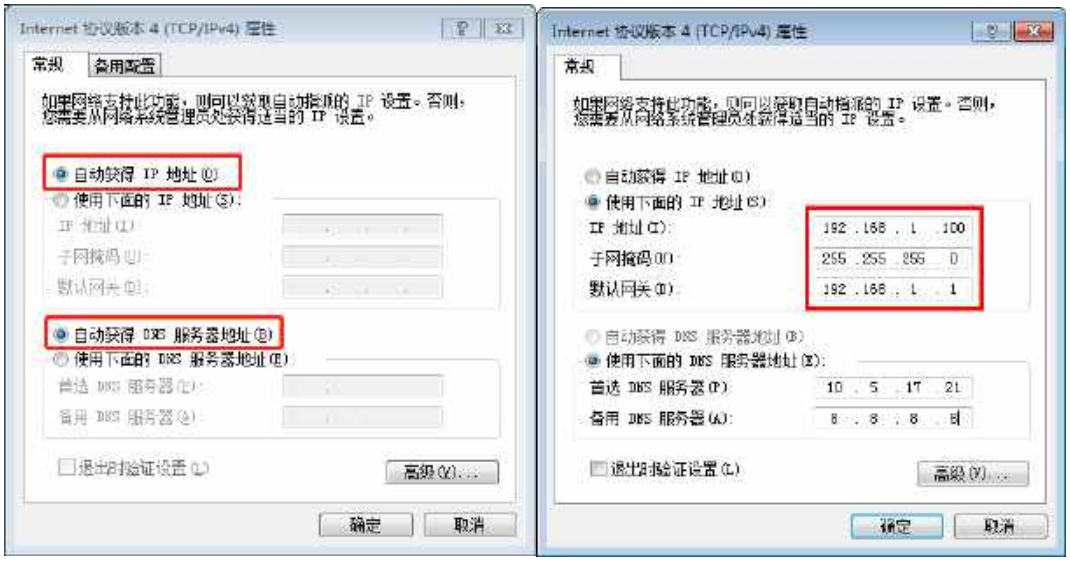
设置 PC 与 InDTU932 设备的 IP 地址在同一网段。

方法一：自动获取 IP 地址（推荐）。

方法二：使用固定 IP 地址，设置 PC 和设备 FE 口在同一网段。设备初始 IP 地址为：192.168.1.1，子网掩码均为 255.255.255.0。选择“使用下面的 IP 地址”，输入 IP 地址（192.168.1.2~192.168.1.254 中任意值），子网掩码（255.255.255.0），默认网关（192.168.1.1），单击确定。

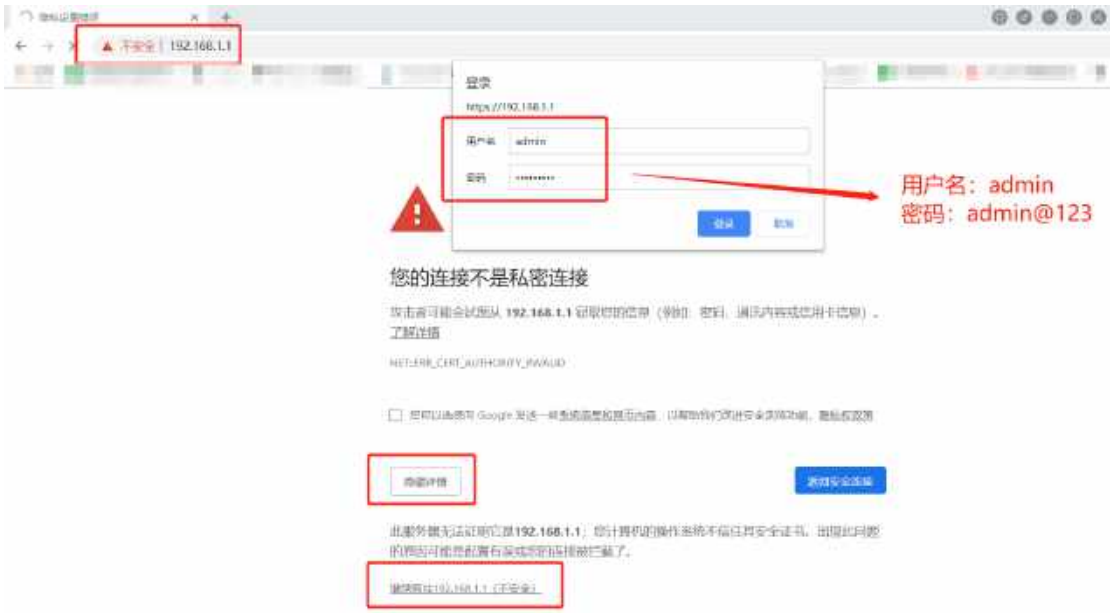
注意：网线接模块的 Ethernet 口，不是 console 口

电脑设置本地动/静态 IP：



2 登录设备

打开浏览器（建议使用谷歌浏览器），输入 https://192.168.1.1 登录（默认出厂是 192.168.1.1），页面会提示不安全，打开隐藏，选择“继续前往”，然后会弹出登录口令，输入 admin/admin@123 登录。



设备支持三种用户：系统管理员，安全管理员，审计管理员

系统管理员(默认：admin/admin@123)：拥有设备全部操作权限，负责设备环境配置，如升级，配置管理，时间管理等；

安全管理员(默认：adconfig/config@123)：负责业务配置，如证书，IPSec，防火墙等；

审计管理员(默认：adaudit/audit@123)：只可查看 log 和基本系统信息。

3 配置设备

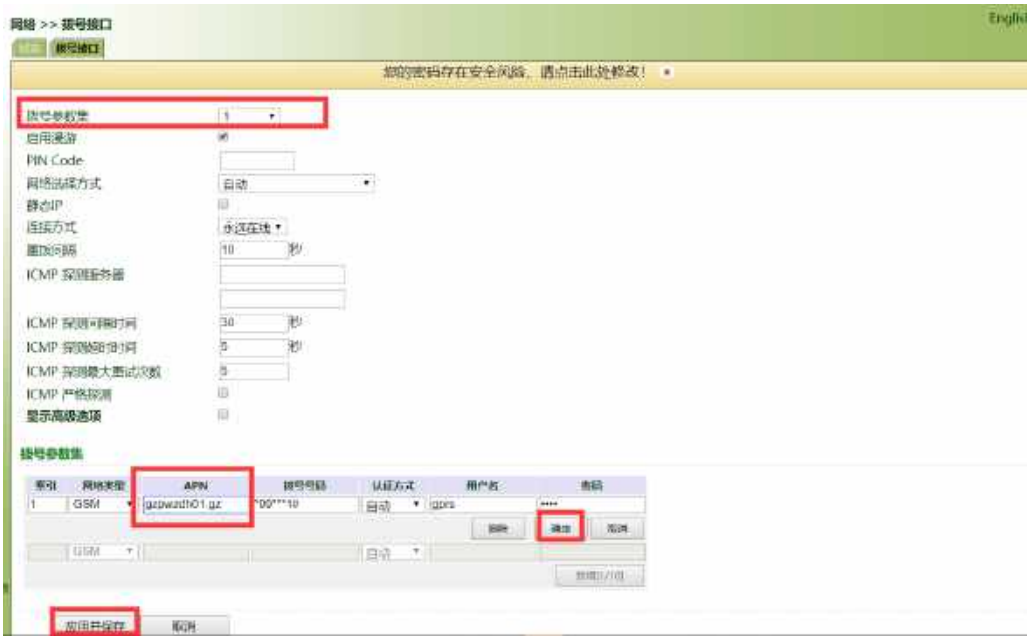
3.1 配置专网卡的参数

点击“网络>>拨号接口>>拨号接口”

进入页面后在最下方有个“拨号参数集”，修改 APN，用户名和密码等信息（一般专网卡都会有 APN，用户名密码如果局方没有提供，就保持默认参数 GPRS，不要修改；拨号号码和认证方式，如果没有特殊需求，也保存默认值），点击确定。

拨号参数集：注意下拉选择对应的拨号参数集，默认是 1

最后点应用并保存，使所有配置保存生效。



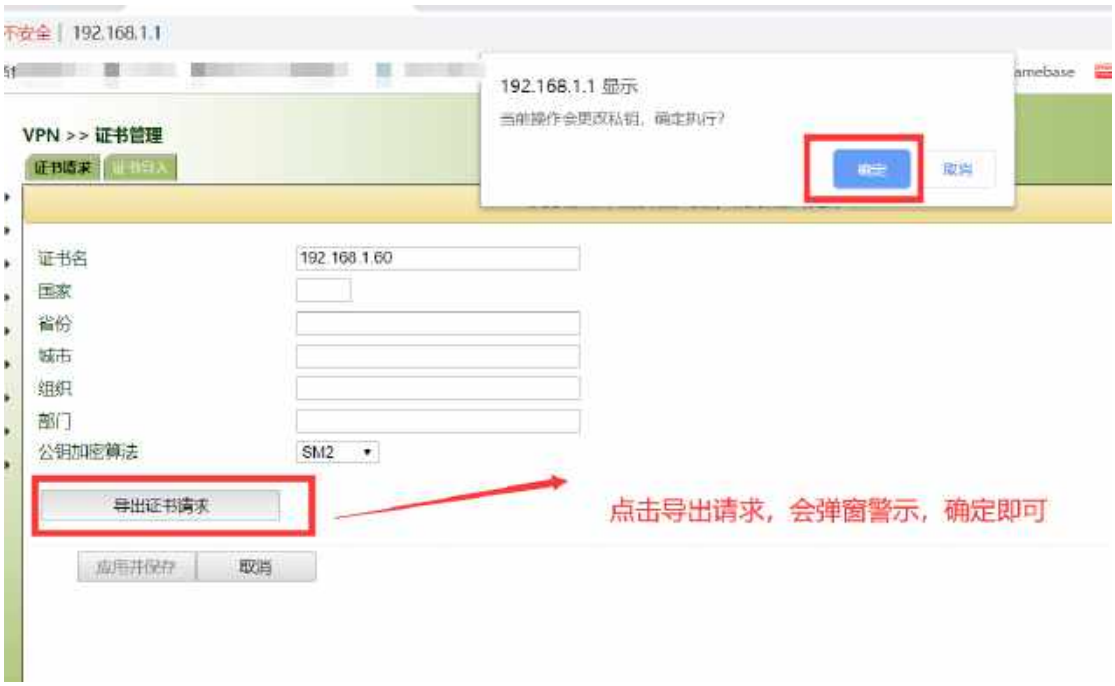
3.2 导出证书文件

点击“VPN>>证书管理>>证书请求”

证书名：按各地主站规划执行，一般以 SIM 卡 IP 命名，其他信息可以不填，留空即可

注意：先填证书名字，再点应用并保存，使证书名字生效。

然后再点导出证书请求，此时浏览器会下载一个证书名.csr 的文件，将此文件发给主站，让其在加密机上签发回来即可。（主站签发回来的证书是 ZIP 格式的压缩包）



关于证书的特别说明：证书都是一对一对使用的，加密模块导出的证书必须要与主站加密机正在使用的证书要相匹配，操作上我们一但导出证书请求后，就不要再次点证书请求，不然会导致证书文件与主站侧不匹配。

3.3 导入证书文件

点击“VPN>>证书管理>>证书导入”

浏览找到主站签发回来的 ZIP 压缩包文件，点击导入证书 ZIP 压缩包，完成后可以看到此

证书相关信息。

3.4 与主站侧加密网关建立IPSEC VPN

建立 IPSEC VPN 目的是加密模块与主站加密机建立加密隧道

IKE V1 隧道与 IPsec 隧道配置按照下图填写即可：

IKEV1 策略：

加密算法：SM1

哈希算法：SM3

生命周期：86400

IPSEC 策略：

封装：ESP

加密算法：SM1

认证方法：SM3

IPsec 模式：隧道模式

注意填完 IKEV1 策略和 IPsec 模式后都要点新增

点击“IPsec 隧道配置>>新增”

新弹出的页面如下配置：

对端地址：主站加密机的 IP 地址

接口名称：cellular

IKEV1 策略：1

IPsec 策略：1

认证方式：数字信封

本地子网：前面填写该 SIM 卡的 IP 地址，后面填写 255.255.255.255（如不清楚该 SIM 卡 IP，可以从模块处查看，）

对端子网：填写允许主站前置机跟加密模块通信的网段，前面是主站前置机的网段，后面是对应的子网掩码；（如果需要建立多个加密通道或同一加密机后有多个子网需要建立隧道，则对端子网处填上多个子网网段即可）

ipsec 协商标准：标准 RFC

所有配置完成后点应用并保存，使配置保存生效。

成功与主站加密机建立 ipsec 通道后，会在状态那显示有一条 tunnel 和 IPsec SA（如果有多条隧道协商成功，则会显示多条 tunnel）

3.5 配置DTU功能

更改加密模块的串口参数，使其跟电力二次设备 DTU/FTU/故障指示器串口参数相匹配

点击“工业接口>>DTU>>串口设置”

这里注意只需要配置串口 1 的参数，串口 2 的不需要更改

我司故障指示器的串口参数是 115200　8　N　1

另外，电力二次设备与加密模块的接线，需要接模块上的 GND TXD1　RXD1

启用 DTU 功能，建立 DTU 功能目的是使得模块能与主站前置机建立 TCP 连接，101 数据能够正常传输到主站侧

DTU 协议：选择透明传输

传输协议：TCP

勾选开启多主站

其次参数可以保存默认

目的 IP 地址：

服务器地址：填写主站前置机的 IP

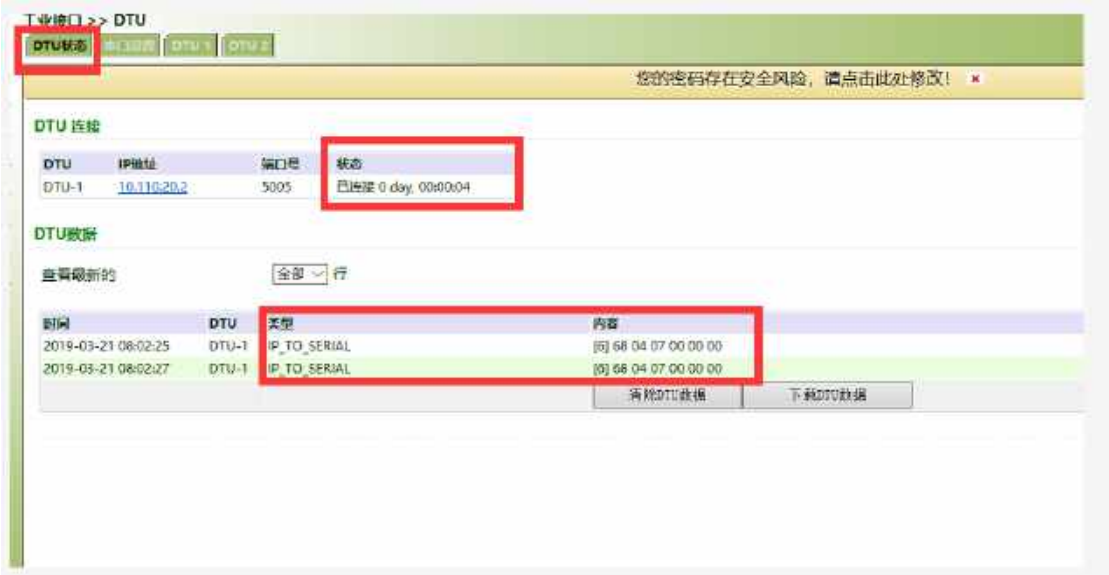
服务器端口：填写主站前置机的端口（这两个参数需要问主站才能确定，一般是要主站先建好通道，确定参数），点新增；如果有多个主站，可以新增多个主站通道信息，每新增一个主站，先点“新增”。

所有配置完成后，点击“应用并保存”，使得本页所有配置生效。

如能正确连上主站前置通道，在“DTU 状态”可以查看到“已连接”信息和 101 报文收发情况。

类型这里：iP_to_serial 代表主站下发的数据，后面内容是具体的数据包

Serial_to_ip 代表电力二次设备上报给主站的数据



3.6 关闭DTU网口

关闭网口的目的是为了进一步降低平均功耗，建议在所有配置完成并且正常连上主站后操作

点击“网络>>以太网接口>>以太网口 0/1”

勾选“关闭”，应用并保存即可

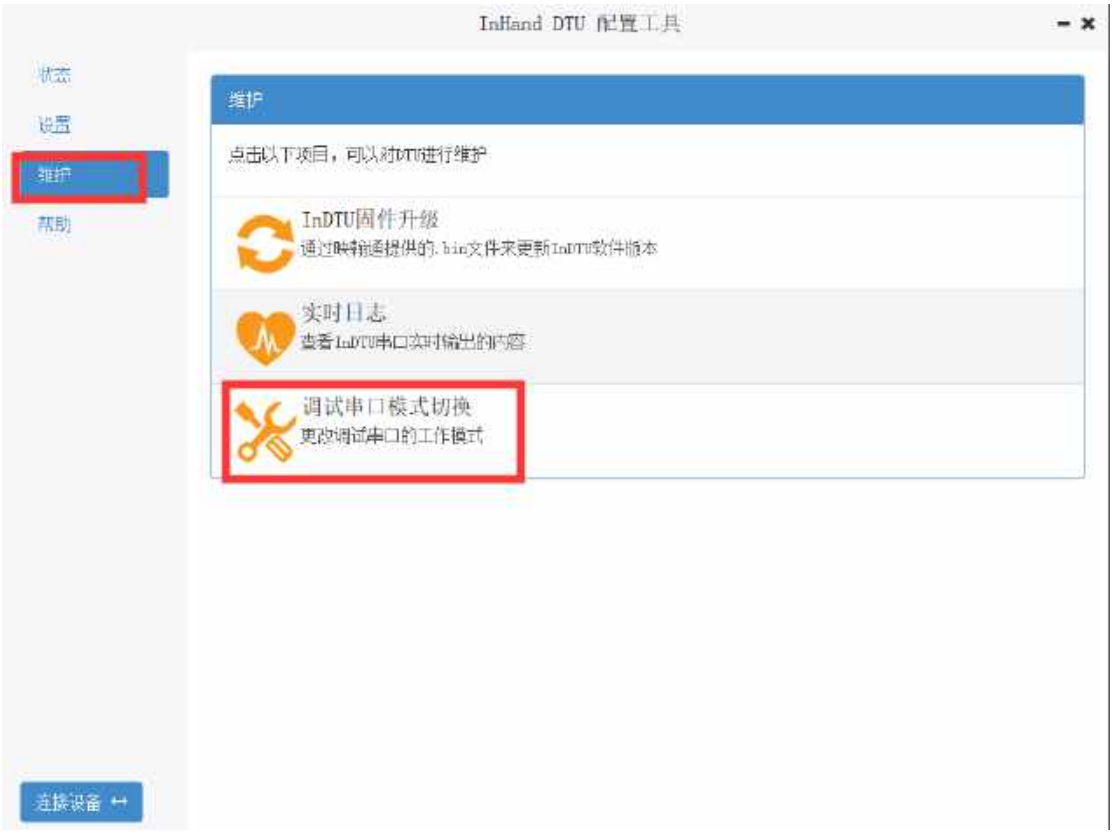
如果在关闭网口后需要重新开启网口，按以下方式操作：

准备 USB 转串口线和 console 调试线，连接到 DTU 的 console 口

电脑打开 

DTUTOOL 软件，选择对应的 COM 口，点“连接”

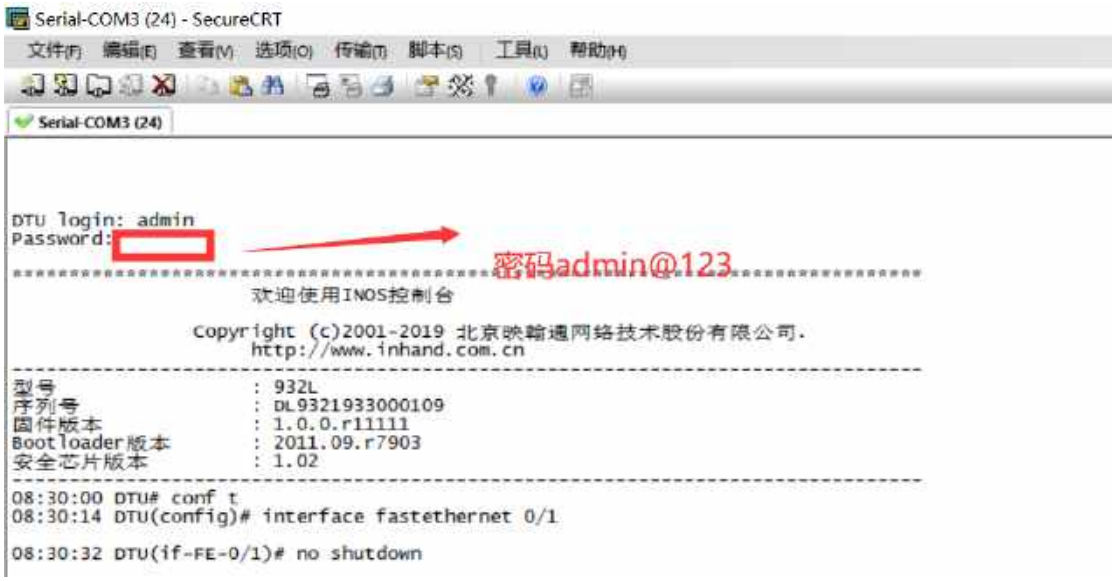
点击“维护>>调试串口切换”，切换到 CLI 模块



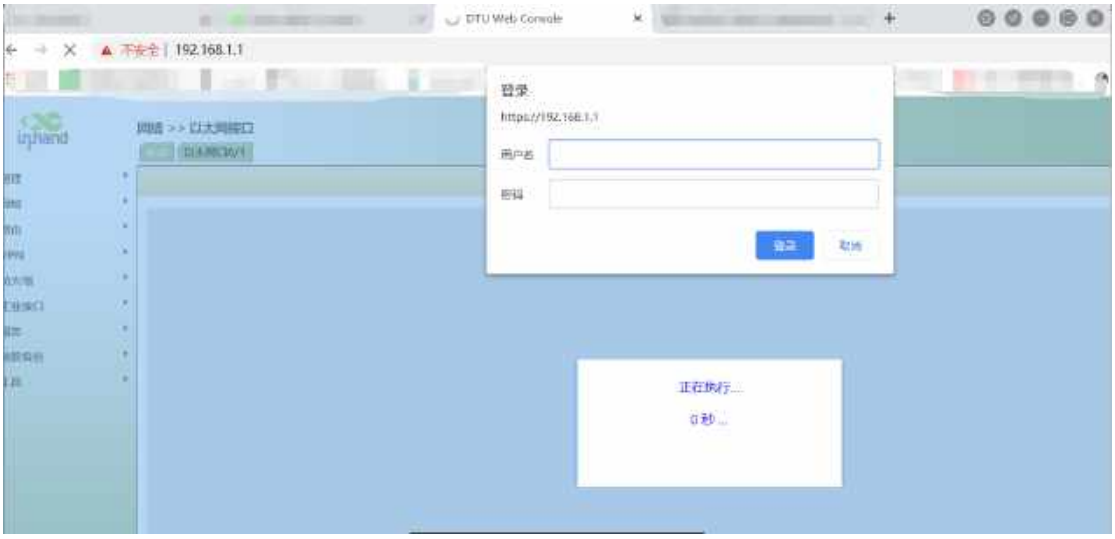
电脑打开SecureCRT 软件，新建快速连接，端口选 USB 转串口线的 COM 号，波特率 115200　数据位 8　无校验　　停止位 1

输入登录用户名 admin　密码 admin@123 登录

在“#”提示符后输入 conf　t，进入 config 模式，输入 interface fastethernet 0/1，进入到 IF-FE-0/1 模式下，输入 no shutdown，回车即可



这时候直接刷新网页又可以正常登录了



4 故障排除

4.1 拨号问题

点击“网络>>拨号接口>>状态”查看当前网络情况，信号值，网络类型，拨号 IP 等信息。

4.2 VPN相关

连接或者 DTU 功能连接失败时，可在“工具>>ping 探测”，输入主站加密机或者前置机的 IP 地址，试试看能否 ping 通，验证网络是否可达

如果最后一行 0%丢失，说明网络可达，反之 100%丢失说明网络不通，此时需要检查 SIM 卡拨号到主站加密机/主站前置机侧网络是否 OK

4.3 其他问题

更多其他情况可以通过下载系统日志方式，提供给我们分析定位问题

点击“管理>>系统日志”，先选择全部日志，点击右下角刷新后，下载日志文件和系统诊断记录，（浏览器会自动下载两个文件）发给我们即可