RISETEK

网·上·先·锋

R5000 系列认证服务器

使用说明书

成都瑞科技术有限公司

目录

1.产品简介

1.1 前言

R5000 系列认证服务器是成都瑞科技术有限公司针对金融、政府、公安等机构对无线网络安全的需求，自主研发的一款针对入网用户进行安全认证的工业级产品。遵循 RADIUS 标准实现身份鉴权，通过综合鉴别 IMSI 号码、用户名和密码，保障用户对自身网络的完整控制权，广泛应用于对无线安全要求较高的行业。

1.2 产品外观

整体外观

前面板

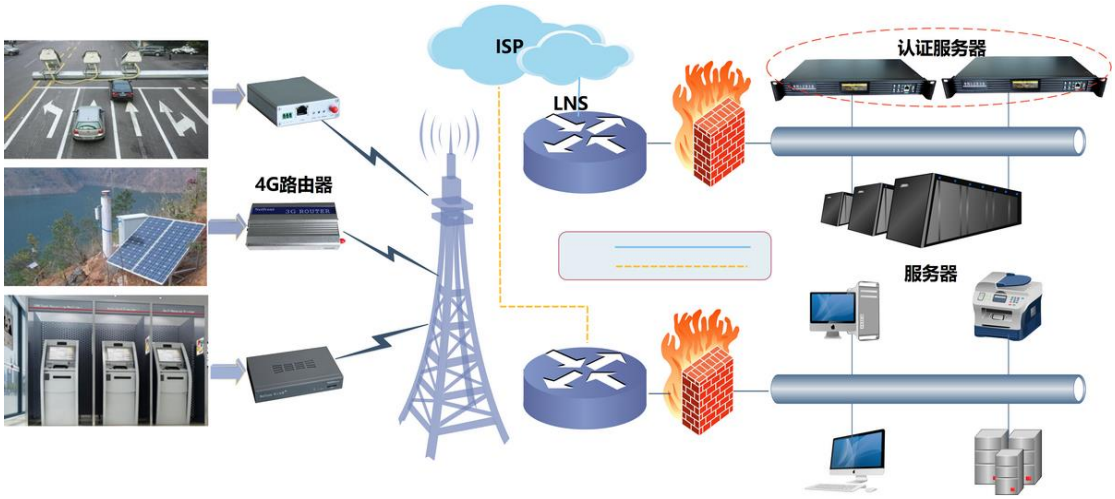
后面板

关于产品详细的物理参数，请参见”R5000系列认证服务器产品介绍说明书”。

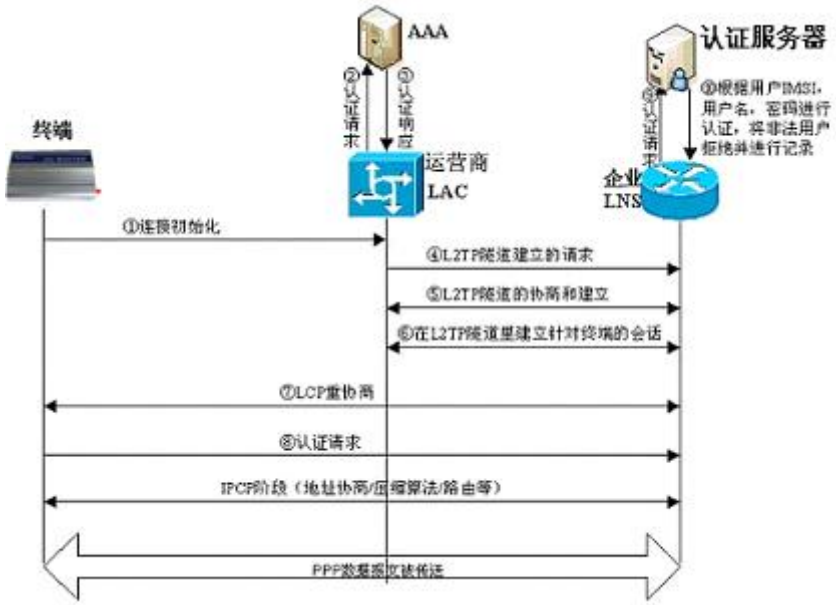
2. 认证服务器原理简述

本节简述认证服务器网络应用图以及系统核心工作流程，关于设备详细的技术指标，请参见“认证服务器技术规范”。

2.1 网络应用图



2.2 工作流程分析



核心工作流程如下：

1、无线终端首先向运营上AAA中心发起连接请求，运营商AAA根据授权情况及时和相应的行业中心建立L2TP隧道，同时把PPP的二次协商直接转向到行业中心。

2、企业LNS向AAA认证服务器发送身份认证请求。

3、AAA认证服务器向企业LNS发送认证结果，如果非法，拒绝请求并记录到相应的黑名单；如果合法，认证通过并进行无线终端设备的IP分配。

3.登录设备

R5000系列认证服务器支持如下三种配置方式，管理员可根据自己的需要和习惯选用。

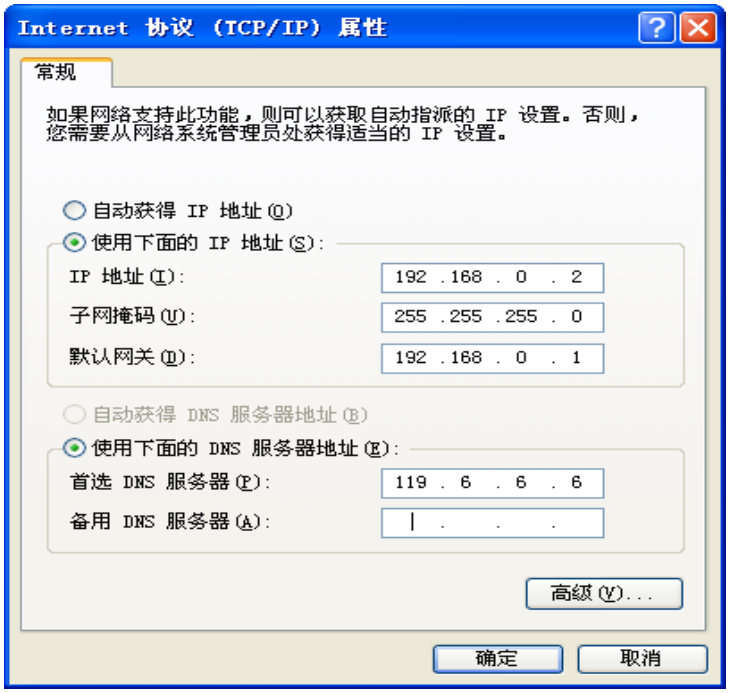
- 基于WEB的管理方式，简单直观、易于操作，推荐使用。下面的配置指导也以此为例。

步骤：

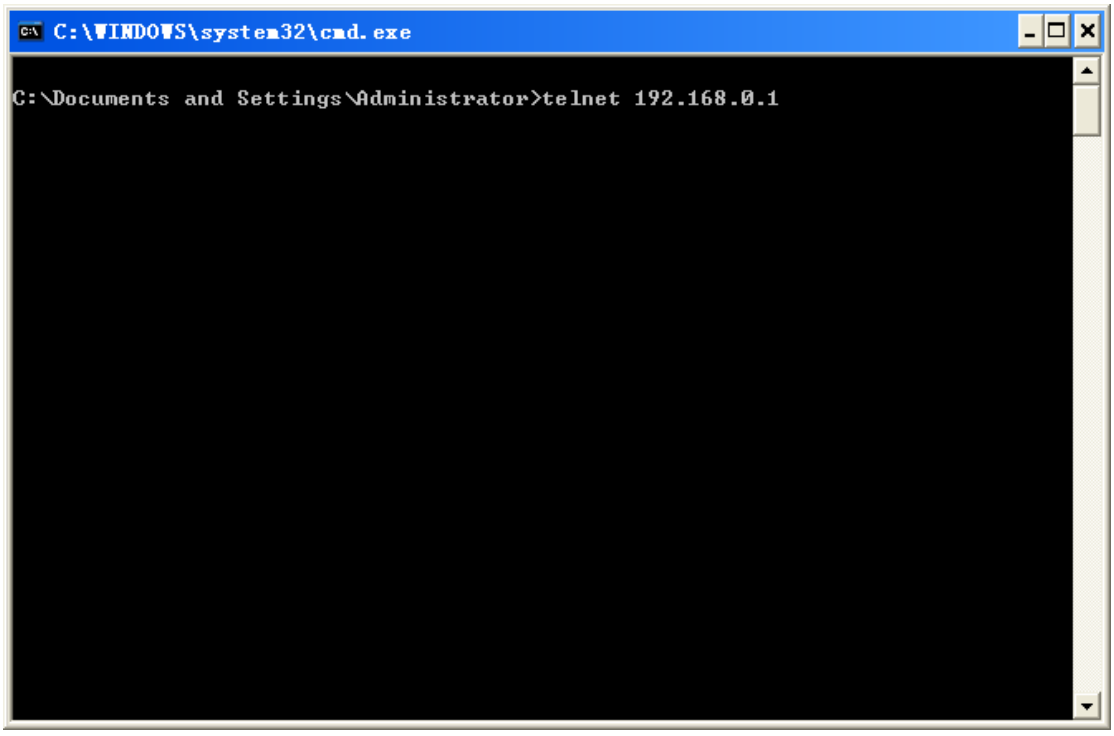
打开浏览器，在地址栏中输入默认IP地址:192.168.0.1，回车后即可进入到认证服务器WEB管理页面。

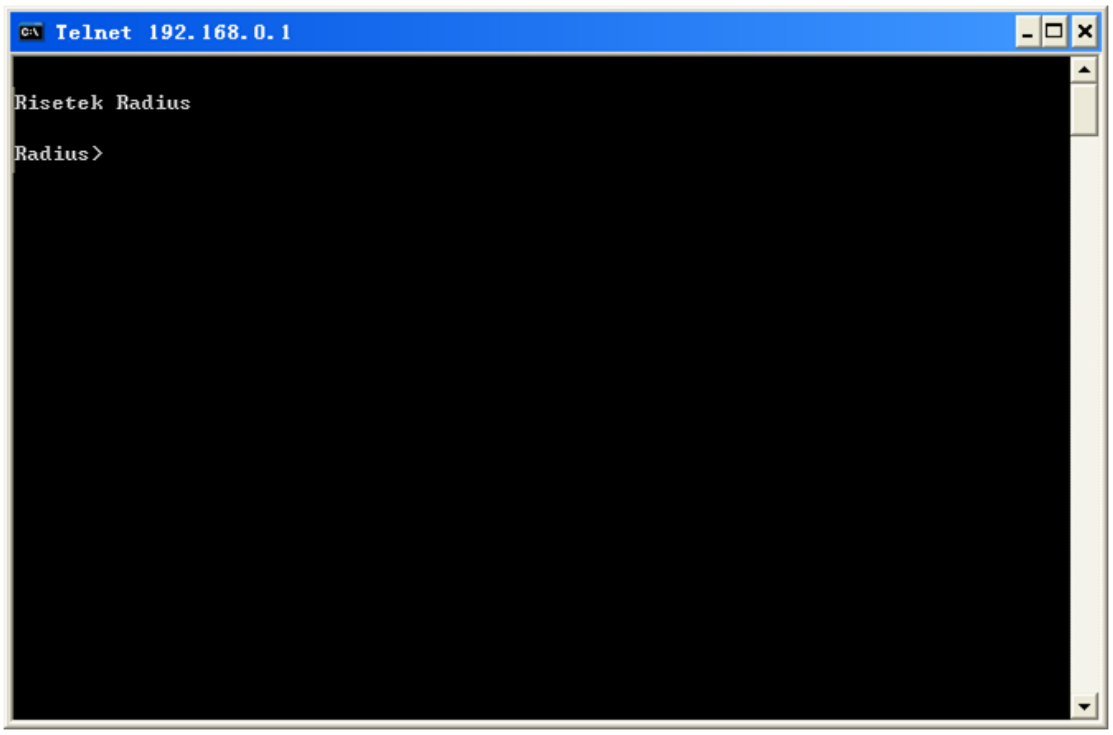
- 通过Telnet进行管理配置

步骤1：用以太网线连接PC和认证服务器后面板的任意一个LAN口，更改PC的IP地址和认证服务器在同一个网段。



步骤2：打开PC的命令提示符窗口，输入：telnet 192.168.0.1，回车后即可登录认证服务器。

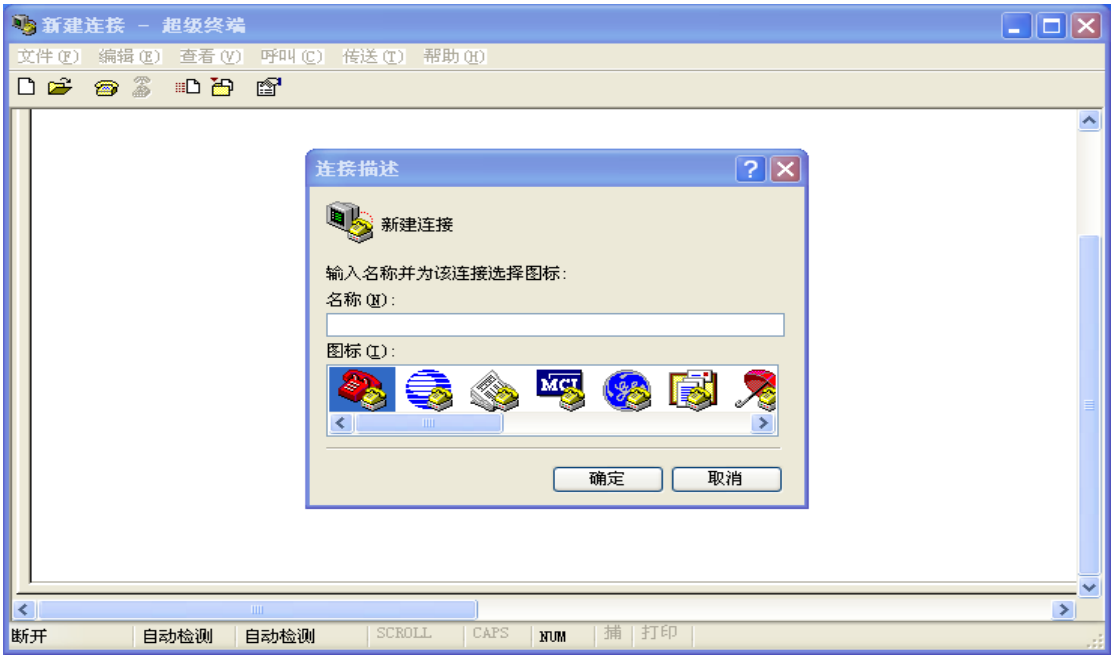


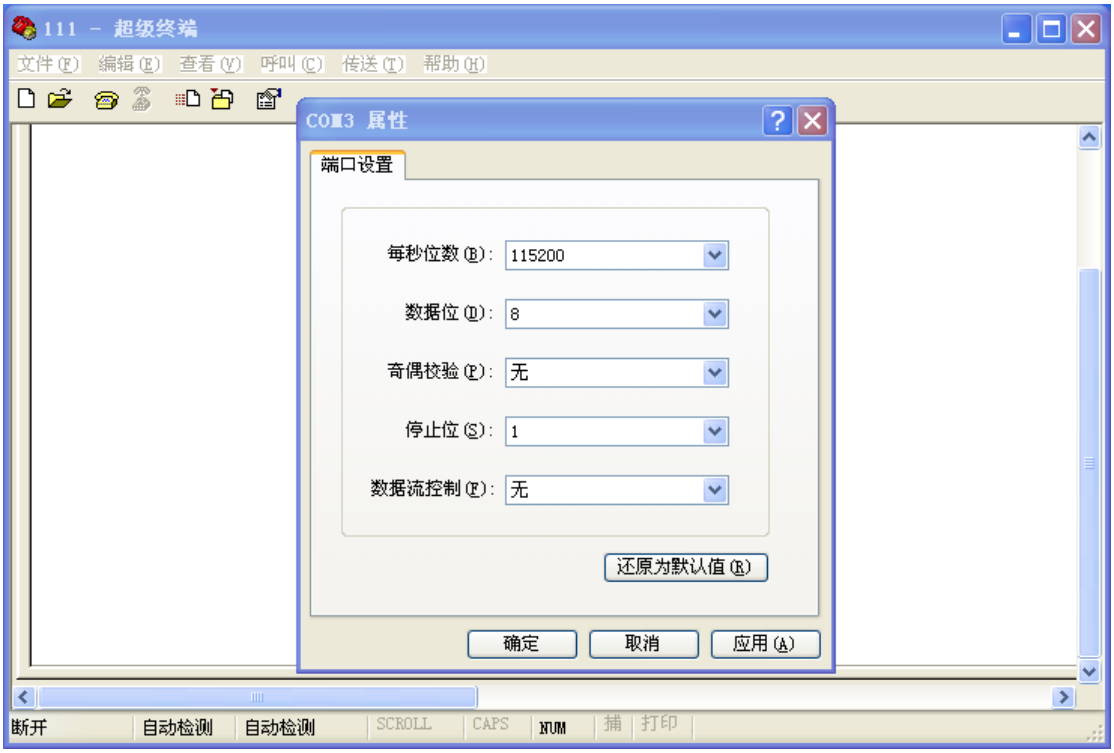


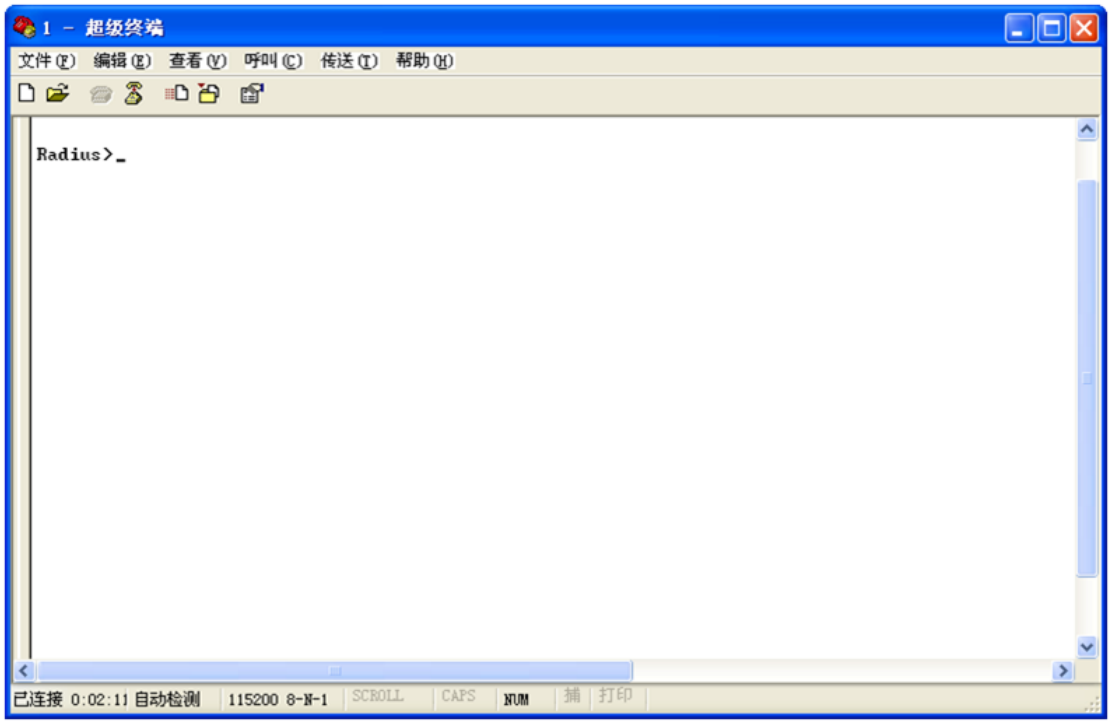
➢ 通过串口进行管理配置

步骤1：使用串口线连接PC的串口和认证服务器前面板上的串口。

步骤2：打开PC的超级终端，选择对应的串口号，设置好波特率，确定后敲回车键即可登录认证服务器。







4.配置指导

4.1 常规配置项

为简化用户管理，配置指导分为常规配置项（必备配置项）和其他配置项（高

级功能配置项/可选配置项），管理员只需配置常规配置项中的几项参数，设备便能正常工作，完成认管理认证功能。

4.1.1 IP 及路由参数配置

1、打开浏览器，地址栏中输入：192.168.0.1（默认地址）进入首页界面，然后点击“**特权登录**”进入配置模式

2、点击菜单栏中“**系统配置**”进入系统配置页面，然后依次点击“**网络配置**”--“**更改**”，填写需要修改的 IP 地址，点击“**更改**”即可。

注：修改 IP 地址后，请在 浏览器中输入新的 IP 地址重新进入。

3、点击“**路由设置**”--“**添加路由**”，在对话框中添加一条指向 LNS 的路由（一般使用一条指向 LNS 的默认路由即可）。

4.1.2 认证配置

点击菜单栏“**认证配置**”，然后可以修改“**鉴权端口**”、“**计费端口**”以及“**共享密钥**”（一般鉴权端口和计费端口不用修改保持默认就好，共享密钥必须和 LNS 上配置的 Radius 认证共享密钥一致）。

4.1.3 不明用户管理

拨号终端发起拨号，LNS 收到会话请求后转发相应的认证信息到认证服务器，管理员可以从不明用户中找到对应用户，通过查看不明用户的终端号和拨号用户名来判断该用户是否为合法用户。如果是，填写用户口令和 IP 地址后，将其导入为合法用户即可；若为非法用户，不予认证。

导入为合法用户操作如下：

点击菜单栏“**不明用户**”，然后点击对应的序号，弹出信息提示框，填写拨号密码和 IP 地址，点击“**导入**”即可。

4.2 其他配置项

4.2.1 配置用户名和密码

基于安全和管理的需要，管理员可以配置登录用户名和密码，点击菜单栏“**系统配置**”--“**管理配置**”--“**添加管理员**”，填写管理员名称和密码，然后点击“**添加**”即完成配置。

4.2.2 添加单个用户

管理员可通过手动添加用户的方式对用户进行预先授权，前提是管理员事先知道拨号用户的终端号码（不同厂家的 LNS 送到认证服务器的终端号码可能不一样，一般是无线数据卡的 IMSI 号码），同时需要预先对拨入用户的拨号用户名、密码、要分配的 IP 地址做好规划。步骤如下：

点击菜单栏“**用户管理**”--“**添加用户**”，填写好对应信息，点击“**添加**”即可。

4.2.3 批量导入用户

在如下情况中，管理员可以使用批量导入用户的功能，节约管理时间。

1）设备更新或更换：从老的认证服务器上导出数据，然后导入到新的认证服务器中。

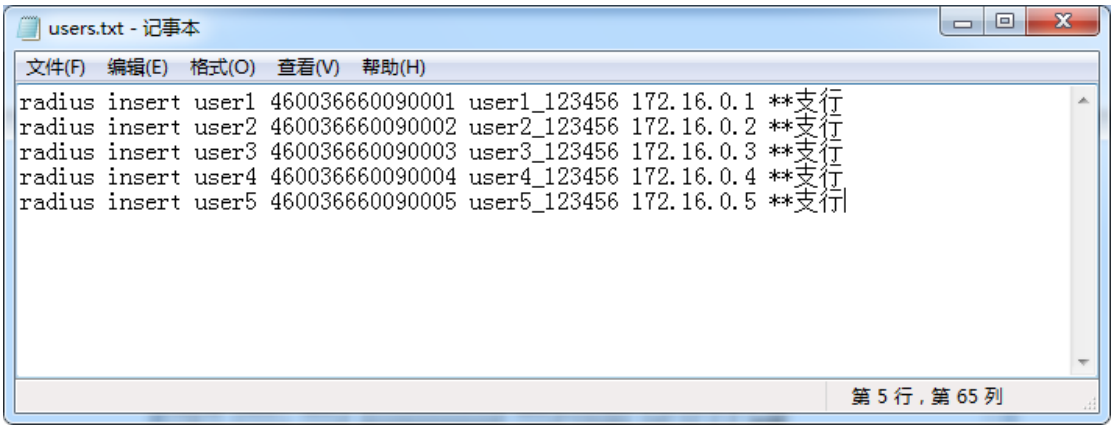
2）主备认证服务器数据同步：将主认证服务器中导出的数据同步到备认证服务器。

3）对即将拨入的大量用户进行预先授权。

使用批量导入功能对用户进行预先授权时，管理员同样需要事先知道拨号用户的终端号码，同时事先对拨入用户的拨号用户名、密码、需要分配的 IP 地址做规划。

批量导入用户数据步骤如下：

1、在记事本中编辑拨号用户信息(若用户数据已存在或已导出，核对无误后即可导入，不再需要编辑)格式如下：



参数说明：

radius insert	固定命令，表示插入用户
user1	拨号用户名，拨号终端上填写的用户名
460036660090001	拨号数据卡的 IMSI 号码
user1_123456	拨号密码，拨号终端上填写的密码
172.16.0.1	给拨号用户分配的固定 IP 地址
**支行	注释，方便管理,可省略该参数

2、使用同步软件（http://www.risetek.com/认证服务器用户数据导入工具.exe 中下载）导入用户数据。

选择用户文件，选中编辑好的 txt 文件，点击“开始同步”后，便开始同步用户数据，同步完成后点击“**用户管理**”可以看到用户已经全部导入。

注：1)认证服务器默认 IP 地址为 192.168.0.1，若 IP 地址已修改，请填写修改后的 IP 地址

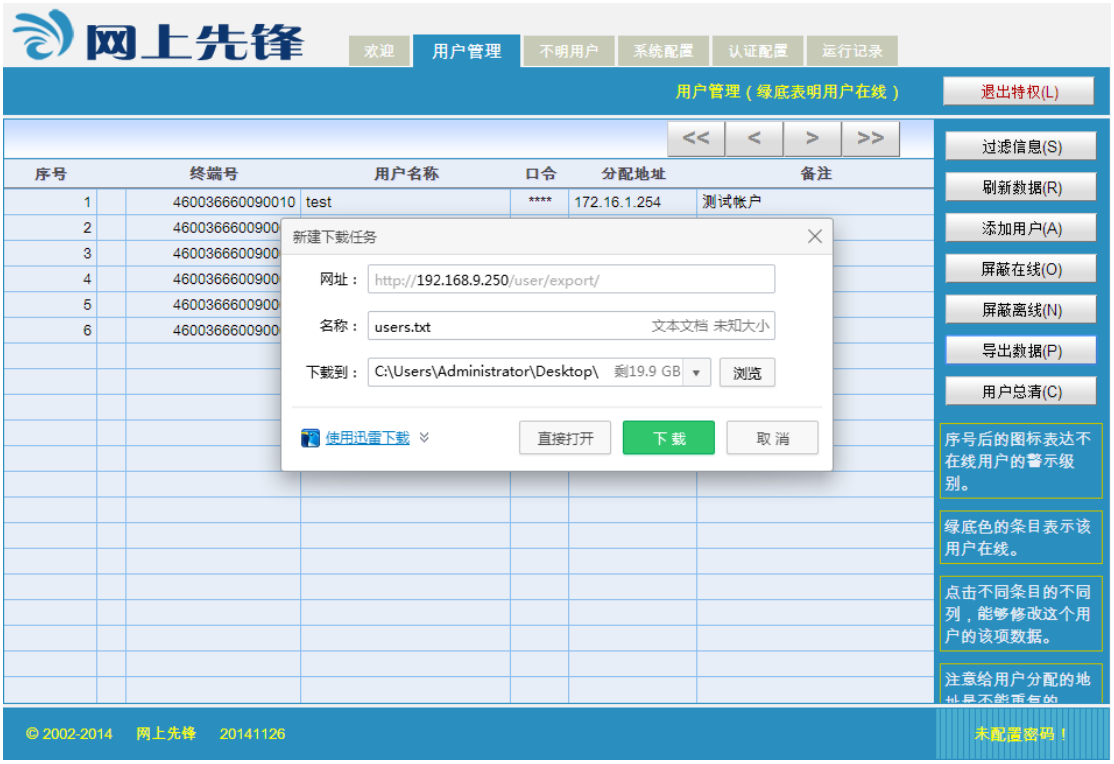
2）若管理员配置了登录用户名、密码以及 enable 密码；请在软件中对应填写，未配置则不需填写。

3）管理员可根据需要启用“保存 log”功能；启用后，导入的每个用户是否成功，从 log 文件里面都看得到。

4.2.4 用户数据导出

若管理员需要备份用户信息或将用户信息导出同步到备认证服务器上，可以使用导出数据功能来实现。

点击“**用户管理**”--“**导出数据**”，然后将用户数据下载到本地即可。



4.2.5 过滤信息

在用户管理和运行记录菜单栏中使用过滤信息功能，管理员可以通过查找关键字很快过滤出需要查找的信息。

点击“**用户管理**”--“**过滤信息**”来实现关键字查找。


网上先锋
欢迎
用户管理
不明用户
系统配置
认证配置
运行记录
用户管理（绿底表明用户在线）
退出特权(L)
<<
<
>
>>
序号
终端号
用户名称
口令
分配地址
备注
1 460036660090010 test **** 172.16.1.254 测试帐户
2 460036660090001 user1 **** 172.16.0.1 **支行
3 460036660090002 user2 **** 172.16.0.2 **支行
4
5
6
设定匹配关键字
Esc|关闭
输入的关键字会匹配记录中的相关数据，空白则清除过滤的限定
9003
确定
取消
过滤信息(S)
刷新数据(R)
添加用户(A)
屏蔽在线(O)
屏蔽离线(N)
导出数据(P)
用户总清(C)
绿底色的条目表示该用户在线。
点击不同条目的不同列，能够修改这个用户的该项数据。
注意给用户分配的地址是不能重复的。
终端号和用户名称的组合确定一个用户，
© 2002-2014 网上先锋 20141126
未配置密码！


网上先锋
欢迎
用户管理
不明用户
系统配置
认证配置
运行记录
用户管理（绿底表明用户在线）
退出特权(L)
<<
<
>
>>
序号
终端号
用户名称
口令
分配地址
备注
4 460036660090003 user3 **** 172.16.0.3 **支行
过滤信息(S)
刷新数据(R)
添加用户(A)
屏蔽在线(O)
屏蔽离线(N)
导出数据(P)
用户总清(C)
绿底色的条目表示该用户在线。
点击不同条目的不同列，能够修改这个用户的该项数据。
注意给用户分配的地址是不能重复的。
终端号和用户名称的组合确定一个用户，
© 2002-2014 网上先锋 20141126
未配置密码！

5. LNS 配置示例

5.1 CISCO 设备作为 LNS 配置示例

```
Building configuration...
Current configuration : 1384 bytes
!
upgrade fpd auto
version 12.2
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
logging rate-limit console 10 except errors
aaa new-model
aaa authentication login default local
aaa authentication ppp default group radius            //设置ppp认证为radius认证
aaa authorization network default group radius         //设置radius授权方式
aaa accounting network default start-stop group radius //设置radius计费方式
enable password 123
!
username aa password 0 123
ip subnet-zero
!
!
no ip finger
!
vpdn enable                                    // L2TP隧道配置
!
vpdn-group vpdn
! Default L2TP VPDN group
 accept-dialin
  protocol l2tp
  virtual-template 1
 lcp renegotiation always                      //重新协商允许
 l2tp tunnel password 0 ****                  //特别重要，L2TP隧道密码从运营商得到。
!
call rsvp-sync
!
```

```
!
interface Loopback0
 ip address 11.0.0.254 255.255.255.255
!
!
interface Ethernet0/0
 ip address 192.X.X.X 255.255.255.0
 half-duplex
!
interface Serial0/0
 ip address 10.X.X.X 255.255.255.X
!
interface Ethernet0/1
 ip address 100.100.100.1 255.255.255.0
 half-duplex
!
!
interface Virtual-Template1              //虚接口，所有拨号设备的WAN接口
 ip unnumbered Ethernet0/0
 no peer default ip address
 compress mppc                           //采用压缩协议，提高效率
 ppp authentication chap pap             //认证方式，优先采用CHAP
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.X.X.X              //指向当地运营商对端地址，保证通信
ip route 192.168.1.0 255.255.255.248 11.0.0.1  //每一个站点的精确路由，特别重要
ip route 192.168.1.8 255.255.255.248 11.0.0.2
ip http server
!
radius-server host 100.100.100.2 auth-port 1812 acct-port 1813 key risetek
                            //指定主认证服务器地址、认证/计费端口、共享密钥
                            注:这里配置的密钥和认证服务器上的共享密钥务必一致
radius-server host 100.100.100.3 auth-port 1812 acct-port 1813 key risetek
                            //指定备认证服务器地址及参数
radius-server retransmit 0
!
line con 0
 transport input none
line aux 0
line vty 5 15
!
no scheduler allocate
end
```

5.2 华为设备作为 LNS 配置示例

```
[V200R003C01SPC300]
#
 snmp-agent local-engineid 800007DB03DCD2FC974449
 snmp-agent
#
 http timeout 3
 http server enable
#
 drop illegal-mac alarm
#
 l2tp enable
#
 wlan ac-global carrier id other ac id 0
#
radius-server template 1                          //配置 radius 服务
 radius-server shared-key simple risetek          //指定密钥，跟认证服务器一致
 radius-server authentication 192.168.4.199 1812 //认证服务器认证地址计费及端口
 radius-server accounting 192.168.4.199 1813      //认证服务器计费地址及端口
#
pki realm default
 enrollment self-signed
#
aaa
 authentication-scheme default
 authentication-scheme l2tp      //配置 aaa 认证方式，方法名为 l2tp(自己随便定义方
                                   法名)
  authentication-mode radius     //认证方式为 radius 认证
 authorization-scheme default
 authorization-scheme l2tp     //配置 aaa 授权方式
 authorization-mode radius     //授权方式为 radius
 accounting-scheme default
 accounting-scheme l2tp      //配置 aaa 审计方式
  accounting-mode radius     //审计方式为 radius
 domain default
 domain default_admin
 domain 3gtest           //指定 isp 域名，下面 interface virtual-template 1 中用到
  authentication-scheme l2tp //指定认证方法为 l2tp
  accounting-scheme l2tp     //指定审计方发为 l2tp
  authorization-scheme l2tp  //指定计费方式为 l2tp
  radius-server 1            //指定 radius 服务模板
 local-user admin password cipher admin
```

```
 local-user admin service-type telnet http
#
firewall zone Local
 priority 16
#
interface Vlanif1
 ip address 192.168.4.254 255.255.255.0
#
interface Ethernet0/0/0
#
interface Ethernet0/0/1
#
interface Ethernet0/0/2
#
interface Ethernet0/0/3
#
interface Ethernet0/0/4
#
interface Ethernet0/0/5
#
interface Ethernet0/0/6
#
interface Ethernet0/0/7
#
interface Ethernet0/0/8
 ip address 221.6.3.2 255.255.255.252  //运营商接入地址
#
interface Virtual-Template1
 ppp authentication-mode chap domain 3gtest
 ip address unnumbered interface LoopBack0
#
interface Cellular0/0/0
 link-protocol ppp
#
interface NULL0
#
interface LoopBack0
 ip address 172.16.1.254 255.255.255.0  //环回接口地址，供虚接口借用
#
l2tp-group 1
 mandatory-chap
 undo tunnel authentication
 allow l2tp virtual-template 1
 tunnel password simple ***     //特别重要，L2TP隧道密码从运营商得到
```

```
#
ip route-static 0.0.0.0 0.0.0.0 221.6.3.1  //指向运营商对端地址后
ip route-static 192.168.1.0 255.255.255.248 11.0.0.1 //每一个站点的精确路由，特
                                                      别重要
ip route-static 192.168.1.8 255.255.255.248 11.0.0.2
#
user-interface con 0
 authentication-mode password
 set authentication password cipher huawei
idle-timeout 0 0
user-interface vty 0
 authentication-mode aaa
 user privilege level 15
user-interface vty 1 4
#
wlan ac
#
return
```

5.3 华三设备作为 LNS 配置示例

```
#
 version 5.20, Release 1808, Standard
#
 sysname H3C
#
 l2tp enable                    //l2tp开启
#
 domain default enable system
#
 telnet server enable
#
 dar p2p signature-file cfa0:/p2p_default.mtd
#
 port-security enable
#
vlan 1
#
radius scheme system
radius scheme vpdntest                  //配置radius（vpdntest是自己定义的）
 primary authentication 22.144.102.8    //认证服务器radius认证地址
 primary accounting 22.144.102.8        //认证服务器radius计费地址
 key authentication risetek             //与认证服务器共享密钥
 key accounting risetek                 //与认证服务器共享密钥
```

```
#
domain tets.vpdn.sc                    //定义domain,一般就定义用户的域名
 authentication ppp radius-scheme vpdntest   //设置ppp认证为radius认证
 authorization ppp radius-scheme vpdntest    //设置radius授权方式
 accounting ppp radius-scheme vpdntest       //设置radius计费方式
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
 accounting optional
domain system
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
traffic behavior behaviorfordeny
 filter deny
#
user-group system
#
local-user admin
 password cipher .]@USE=B,53Q=^Q`MAF4<1!!
 authorization-attribute level 3
 service-type telnet
#
l2tp-group 1
 mandatory-chap
 allow l2tp virtual-template 1
 tunnel password simple dxvpdn          //特别重要，L2TP隧道密码从运营商得到。
#
interface Aux0
 async mode flow
 link-protocol ppp
#
interface Virtual-Template1
 ppp authentication-mode chap domain cc_zxyh.vpdn.jl
 ip address unnumbered interface LoopBack0
#
interface NULL0
#
interface LoopBack0
 ip address 11.0.0.254 255.255.255.255
#
```

```
interface GigabitEthernet0/0
 port link-mode route
 ip address 10.232.2.106 255.255.255.252        //当地运营商接入地址
#
interface GigabitEthernet0/1
 port link-mode route
 ip address 192.168.2.1 255.255.255.0              //用户内网地址
#
 ip route-static 0.0.0.0 0.0.0.0 10.232.2.105     //指向当地运营商对端地址
 ip route-static 192.168.1.0 255.255.255.248 11.0.0.1 //每一个站点的精确路由，特
                                                      别重要
 ip route-static 192.168.1.8 255.255.255.248 11.0.0.2
#
 load tr069-configuration
#
user-interface con 0
user-interface aux 0
user-interface vty 0 4
 user privilege level 3
 set authentication password cipher admin123
#
return
```

6. 常见故障现象及处理

6.1 能 ping 通认证服务器 IP,网页不能打开

1、大多数情况下，管理员都不是直接使用电脑和认证服务器连接，而是通过远程的方式来进行操作。若中间是否经过了防火墙等安全设备，请先检查防火墙策略。

2、请尝试更换浏览器进行问题排查，推荐使用 google 公司的 Chrome 浏览器。

3、请尝试使用计算机通过网线直接连接认证服务器（本地管理）进一步排除问题。

4、若计算机直连认证服务器问题还是存在，请更换浏览器或者更改浏览器设置

1）推荐使用 google 公司的 Chrome 浏览器

2）360 浏览器，把兼容模式改为极速模式

3）sogo 浏览器，启用高速模式

4）IE 浏览器，启用兼容性视图

5、联系厂家技术支持

6.2 认证服务器收不到任何信息

1、请检查配置是否正确，包括 LNS 配置以及认证服务器配置。

2、确认 LNS 和认证服务器之间的网络可达，若中间存在防火墙等安全设备，请检查防火墙策略是否放行 radius 相关的协议。

注：上面两点测试，可以通过在 LNS 上输入命令进行 3A 测试的方式检查配置以及连通性。

思科设备命令：Router#test aaa group radius test test new-code

华为设备命令：<Huawei>test admin 123456 radius-template 1