RG-UAC 6000 系列统一上网行为管理与审计系统产品命令手册

版权声明

免责声明

本手册内容依据现有信息制作，由于产品版本升级或其他原因，其内容有可能变更。锐捷网络保留在没有任何通知或者提示的情况下对手册内容进行修改的权利。

本手册仅作为使用指导，锐捷网络在编写本手册时已尽力保证其内容准确可靠，但并不确保手册内容完全没有错误或遗漏，本手册中的所有信息也不构成任何明示或暗示的担保。

目录

1 系统综述

系统概述

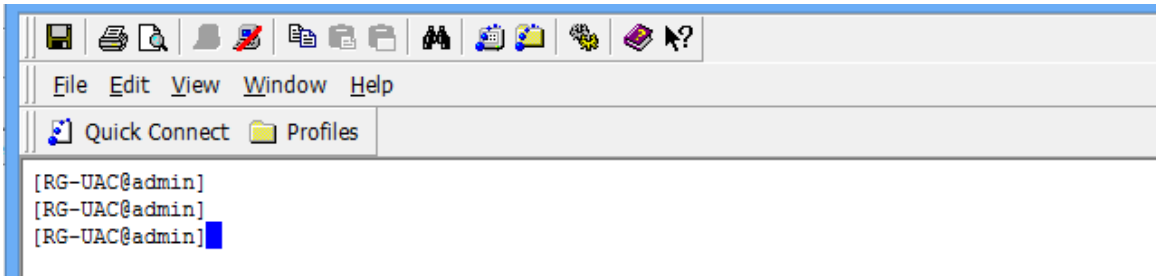
RG-UAC 系统可以通过命令行配置，也可以通过图形界面进行配置。其中命令行配置除了可以通过 console 口连接，也可以通过 SSH 连接，图形界面采用的 B/S 模式，可以通过 HTTPS 和 HTTP 进行连接。本手册只介绍通过命令行的方式进行配置管理。

1.1 命令行特性

这一节主要讲述当您进入命令行进行配置时所要进行的步骤。请仔细阅读本节以及后边几节中关于使用命令行接口的详细信息。

使用命令行接口（CLI），请按照以下步骤：

第 1 步：当进入命令行接口出现命令提示符后，请确认您有相应的权限。大多数配置命令都需要用户您有管理员权限。



root 说明使用者是超级管理员

第 2 步：键入命令名称。

如果命令不含需要用户输入的参数，那么请直接跳到第 3 步。如果命令含需要用户输入的参数，那么继续以下步骤：

1）如果命令需要一个参数值，请输入一个参数值。在输入参数值时，可能要输入关键字。

2）命令的参数值部分一般指定了您应该输入什么样的参数，是某范围内的数值，或者字符串或者 IP 地址。关键字是指命令中要操作的对象。

3）如果命令需要多个参数值，请按命令的提示依次输入关键字和每个参数值。直到提示信息中出现让您按回车键信息为止。

第 3 步：输入完整的命令后，请按回车键。

例如：“exit” 是一个不含参数和关键字的命令。命令名称为 exit；“ip address A.B.C.D/M” 是一个

含有参数和关键字的命令。其中命令名称为 ip，关键字为 address，参数值为 A.B.C.D/M。

1.1.1 语法帮助

命令行接口内置有语法帮助。如果您对某个命令的语法不是很确定，请输入该命令中您所知道的部分，然后输入“--help”。命令行会提示您已经输入的部分命令后剩余部分的可能的命令清单。

```
# ls --help
BusyBox v1.13.3 (2014-03-13 16:01:46 CST) multi-call binary

Usage: ls [-1AacCdeFilnpLRrSsTtuvwxXhk] [filenames...]

List directory contents

Options:
        -1      List in a single column
        -A      Don't list . and ..
        -a      Don't hide entries starting with .
        -C      List by columns
        -c      With -l: sort by ctime
        --color[={always,never,auto}]   Control coloring
        -d      List directory entries instead of contents
        -e      List full date and time
        -F      Append indicator (one of */=@|) to entries
        -i      List inode numbers
        -l      Long listing format
        -n      List numeric UIDs and GIDs instead of names
        -p      Append indicator (one of /=@|) to entries
        -L      List entries pointed to by symlinks
        -R      List subdirectories recursively
        -r      Sort in reverse order
        -S      Sort by file size
        -s      List the size of each file, in blocks
        -T NUM  Assume tabstop every NUM columns
        -t      With -l: sort by modification time
        -u      With -l: sort by access time
        -v      Sort by version
        -w NUM  Assume the terminal is NUM columns wide
        -x      List by lines
        -X      Sort by extension
        -h      List sizes in human readable format (1K 243M 2
G)

# 
```

1.1.2 使用语法帮助补齐命令

系统提供用户输入“Tab”键后，对命令进行补齐的功能。当您输入了一部分命令后，再输入“Tab”键，如果匹配的命令有多个，则列出可能的命令清单，如果匹配的命令只有一个，那么命令行会自动把用户输入的那部分命令补齐，并把光标移至最后。

```
[HOSTNAME@root]ls
ls       lsattr  lsmod   lspci
[HOSTNAME@root]ls
```

按 Tab 后补齐命令

1.1.3 命令中的符号

您可能会在命令语法中看到各种符号，这些符号只是说明您该如何输入该命令，但是不是命令本身的一个部分。下表对这些符号进行了概要说明。

表 1-1 命令行中的符号

符号	描述
通配符" * ” 、" ? ”	和DOS下一样，当我们不知道确切的文件名时，可以用通配符来进行模糊操作。“*”可以代表任意长度的任意字符，“?”代表一个任意字符。 例如命令： 列出以.awk 结尾文件的详细信息 ls -l *.awk
转义字符“\”	如果要操作的文件名中包含有这些特殊符号，我们可以结合“\”来表达。 例如命令： 匹配" * ” 字符 *
目录:"/”、"~”、"." 、"..”	它们分别代表的意思是： " / ” ：根目录(在中间使用表示路径) "~ ” ：用户根目录(用户登录时所在的目录) " . ” ：当前目录

符号	描述
	".." ：上级目录 例如命令： 切换到根目录 cd /
管道和重定向："＞"、"＞＞"、"＜"、"|"	重定向就是使命令改变它所认定的标准输出。 例如命令： cat data1.txt＞＞data2.txt 将data1.txt文件的内容加在data2.txt文件的后面
# 井号	脚本文件运行时，使用的解释器。 #!/bin/sh 其他时候表示注释

1.2 实现系统配置的途径

您可以通过以下途径对设备进行管理：

- 使用终端(或者仿终端软件)连接到设备的串口(Console)从而访问设备的命令行接口(CLI)
- 使用 SSH 管理设备

1.2.1 通过串口实现系统配置

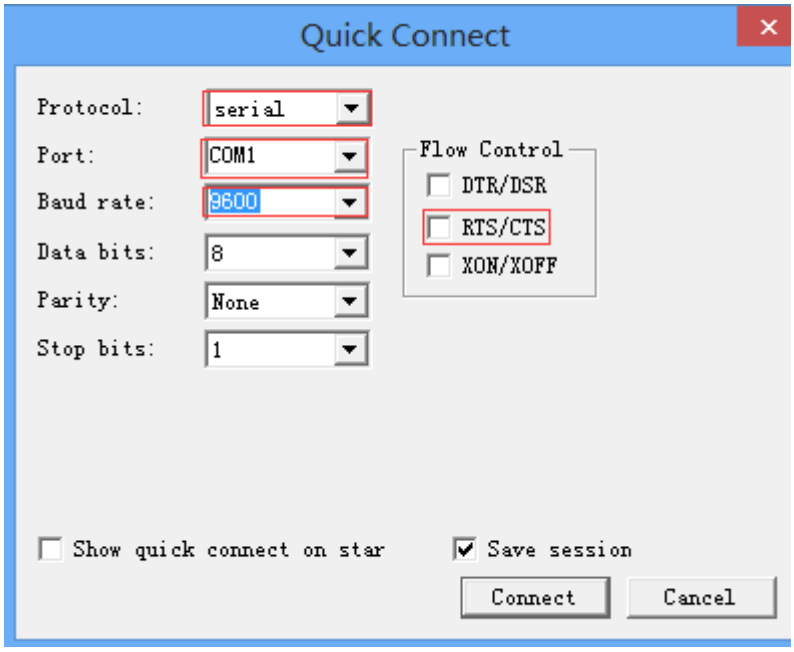
- 波特率 ：9600
- 数据位 ：8
- 奇偶校验：无

- 停止位 ：1
- 流量控制：无

正确设置完 Console 的参数并将设备加电，可以看到设备的登录提示信息。

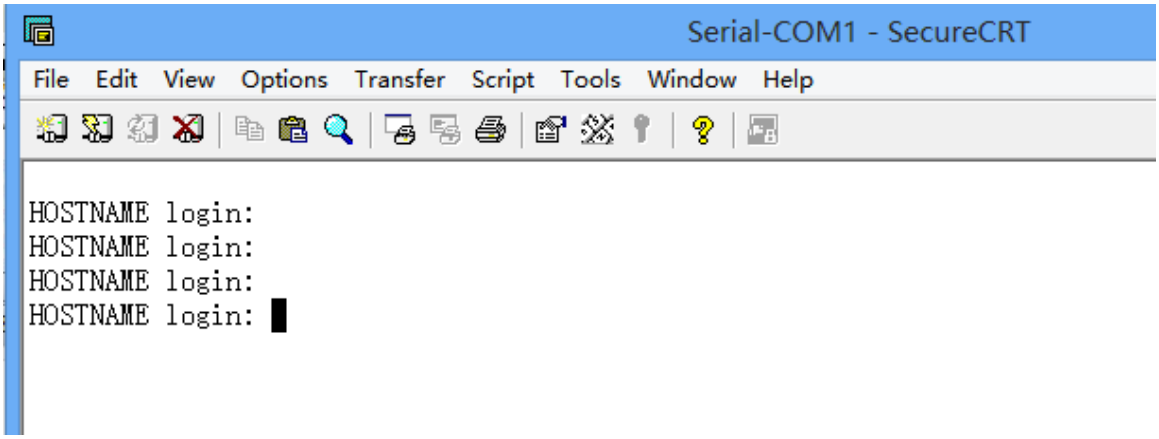
行为管理设备串口登录方法

1、 打开 SecureCRT 软件，选择【文件—快速连接】，弹出如下图对话框，并按下面的对话框配置好：



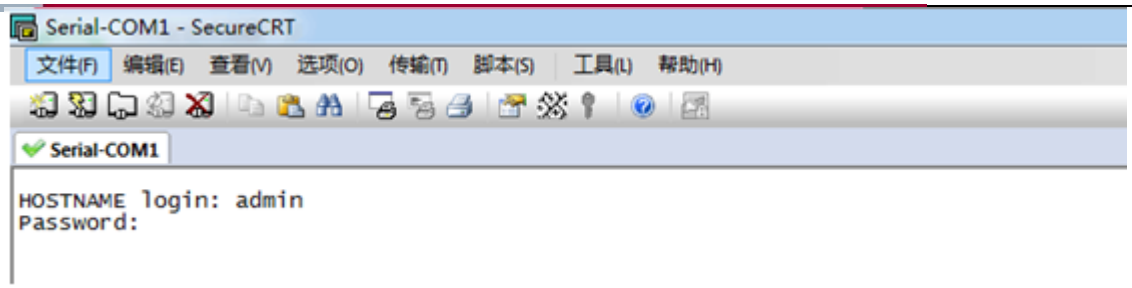
上图中参数设置必须要与红框上的设置一致，其他参数采用默认的即可；

2、选择上图中的“连接”按钮，并敲回车，出现如下图：

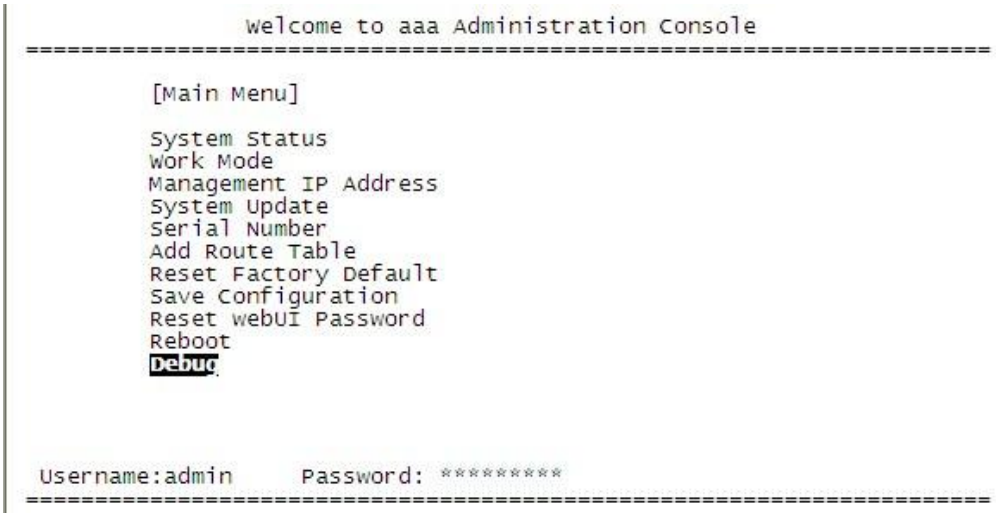


在此页面上面输入第一级用户名：admin

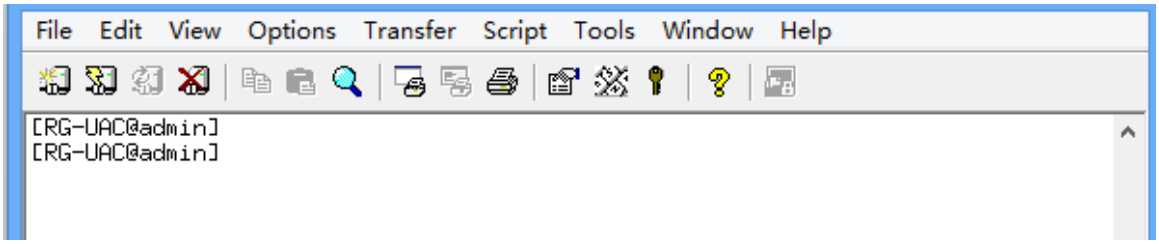
回车输入第一级密码：firewall **（注：如果 web 页面的 admin 用户密码修改，则会跟着修改该后台密码）**(此密码在输入时 scrt 上无显示)，如下图所示：



在上图中用上下方向键选择 Debug 按钮，回车，并要求输入第二级用户名及密码，如下页面所示：



第二级用户名为 admin，密码是 Login*PWD；输入完成后即可进入到命令行下，如下图所示：



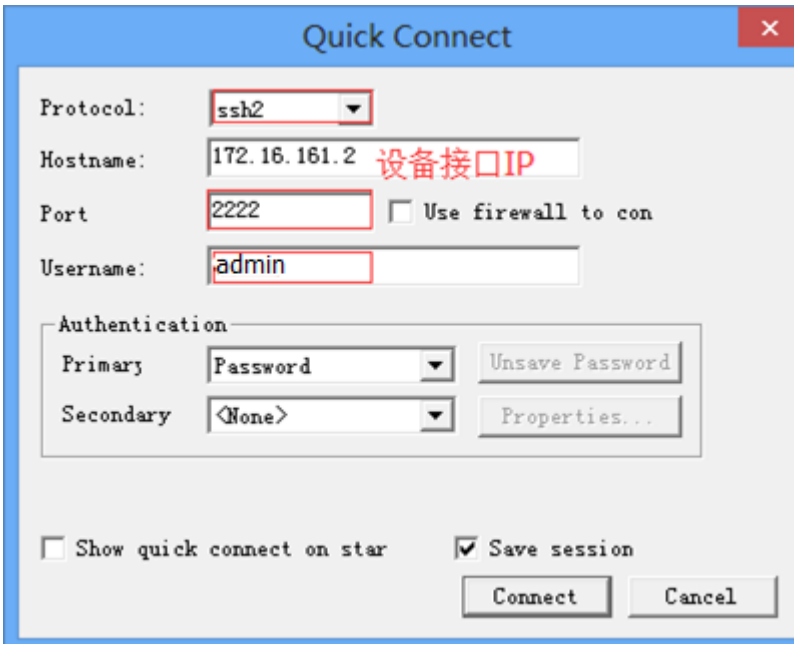
在此命令行下可进行相关命令的操作。

1.2.2 通过SSH方式实现系统配置

网络被攻击，很多情况是由于服务器提供了 Telnet 服务引起的。Telnet 服务有一个致命的弱点——它以明文的方式传输用户名及口令，所以，很容易被别有用心的人窃取口令。目前，一种有效代替 Telnet 服务的有用工具就是 SSH 服务。SSH 客户端与服务器端通讯时，用户名及口令均进行了加密，有效防止了对口令的窃听。设备支持以 SSH 的方式对设备的管理。

任何一个有 SSH 功能的工作站都能通过 TCP/IP 网络连接到设备。可以通过以下步骤登录到设备：

1. 打开 SecureCRT 软件，选择【文件—快速连接】，弹出如下图对话框，并按下面的对话框配置好：



上图中参数设置必须要与红框上的设置一致，其他参数采用默认的即可；

2. 选择上图中的“连接”按钮，并敲回车，出现如下图：

用户名:admin

密码：firewall **（注：如果 web 页面的 admin 用户密码修改，则会跟着修改该后台密码）**

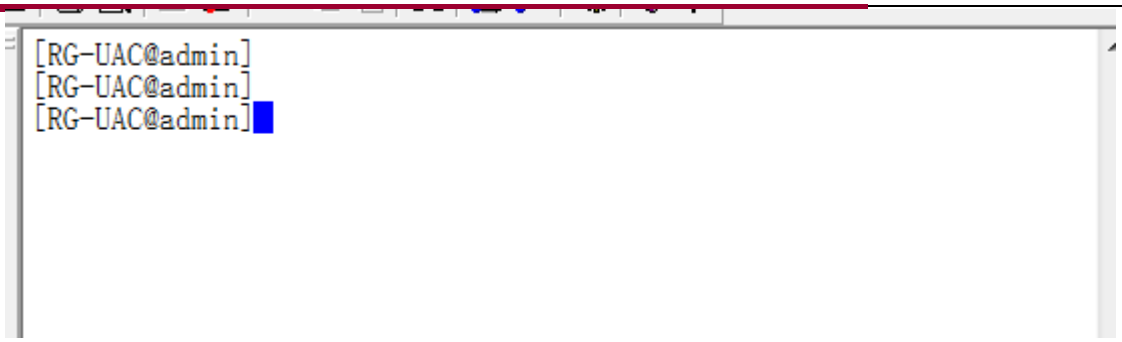
3. 密码输入之后，敲回车，进入如下页面：

```
                Welcome to test Administration Console
 ================================================================
=====
          [Main Menu]

          System Status
          Serial Number
          Version Information
          Work Mode
          Management IP Address
          System Update
          Download Debug information
          Add Route Table
          Reset Factory Default
          Save Configuration
          Reset WebUI Password & Management Policy
          Reboot
          Debug


 ----------------------------------------------------------------
```

4. 在上图中用上下方向键选择 Debug 按钮，回车，并要求输入第二级用户名及密码，如下页面所示：

```
                Welcome to test Administration Console
 ================================================================

          [Main Menu]

          System Status
          Serial Number
          Version Information
          Work Mode
          Management IP Address
          System Update
          Download Debug information
          Add Route Table
          Reset Factory Default
          Save Configuration
          Reset WebUI Password & Management Policy
          Reboot
          Debug


 Username:admin      Password: *********  Login*PWD
 ================================================================
```

5. 第二级用户名为 admin，密码是 Login*PWD；输入完成后即可进入到命令行下，如下图所示：

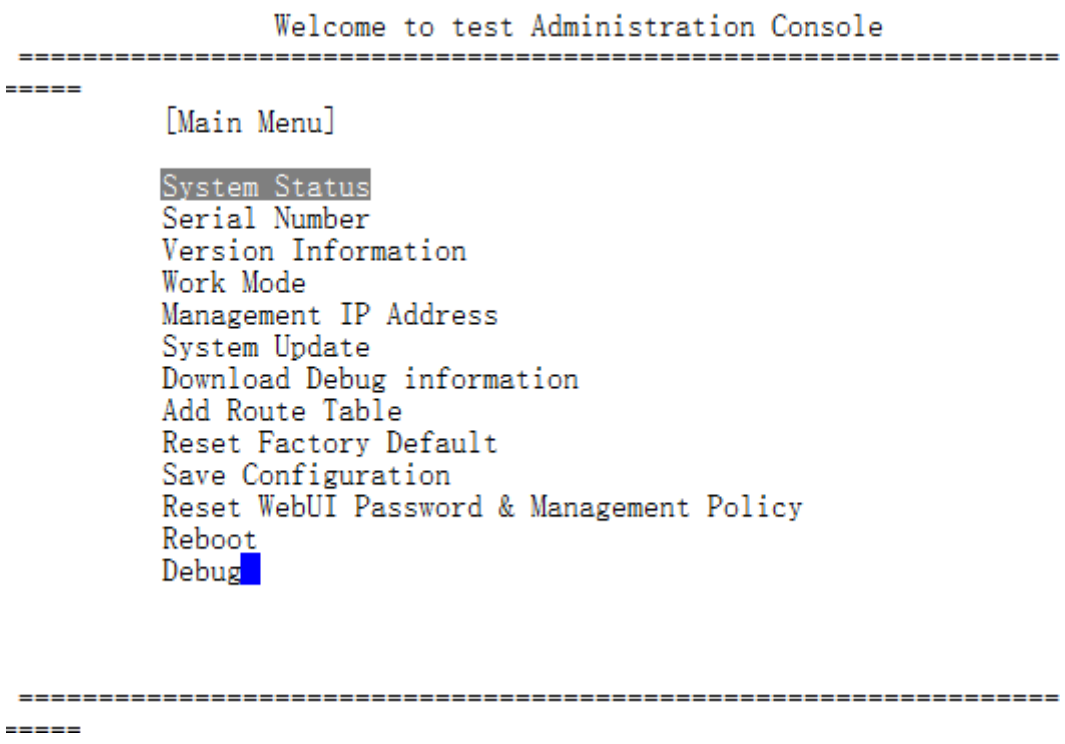


此命令行可进行相关命令的操作。

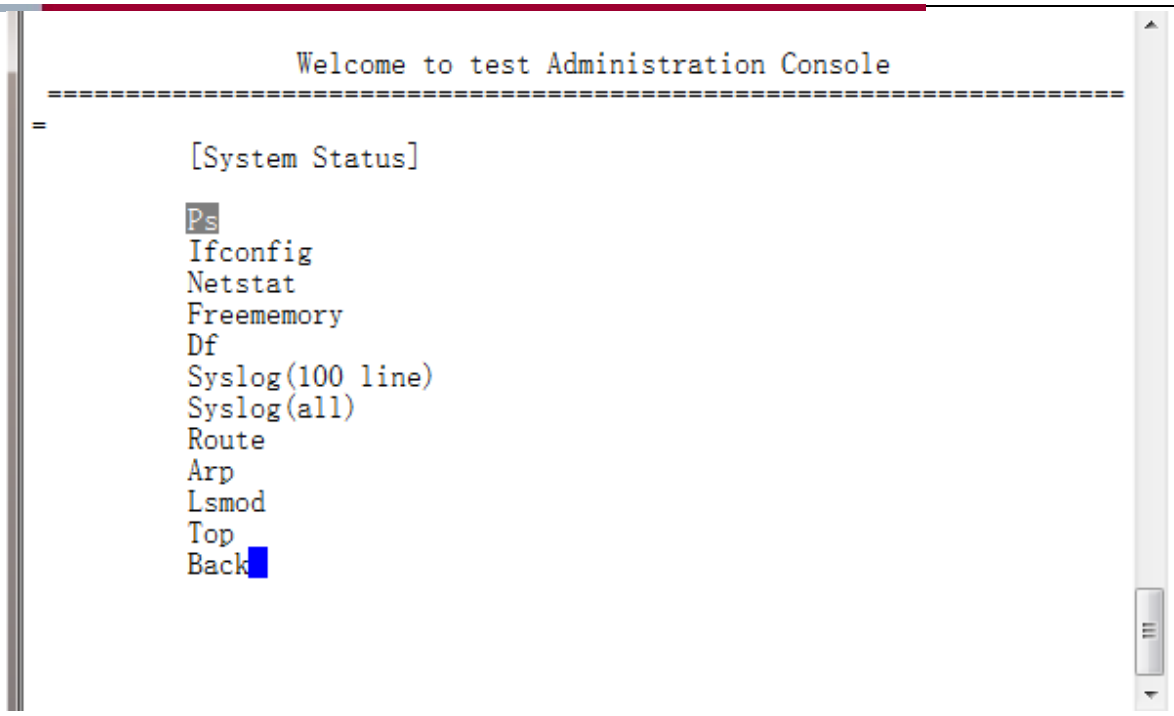
1.3 常用系统管理命令

1.3.1 查看当前系统的运行状态

后台一级密码登陆，选择菜单 System Status

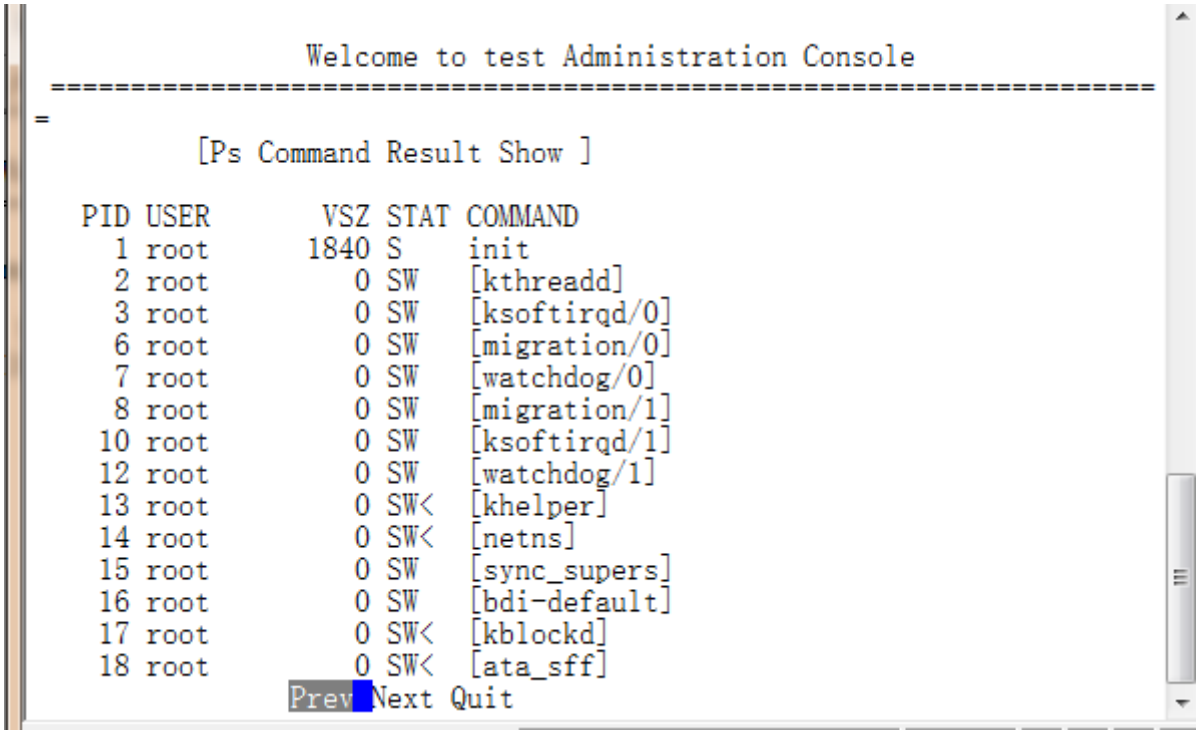


按回车键



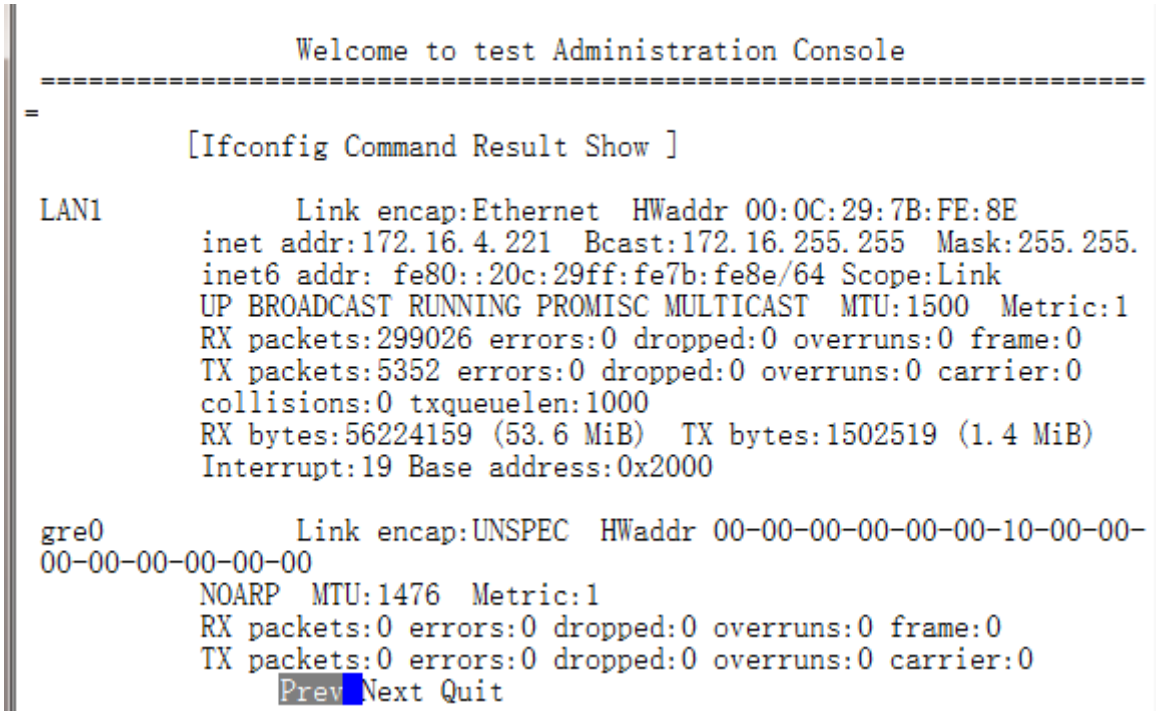
可选择一些简单的命令查看当前系统状态。使用上下键进行移动，选中后使用回车键进入命令行，查看详细信息。

Ps：可查看当前系统中运行的所有程序。如下图所示：



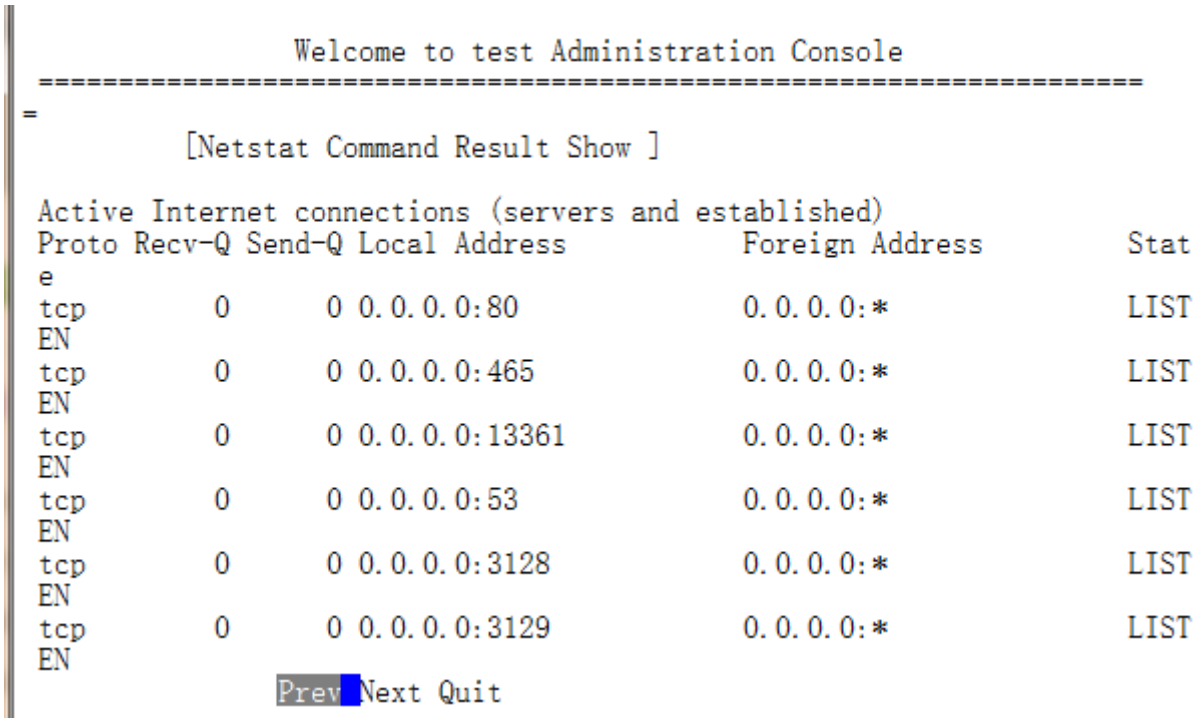
可使用 Prev 和 Next 按纽进行翻页，Prev 是往前翻，Next 是往后翻；可用 Quit 退出 ps 命令行。使用左右键进行移动。

Ifconfig：查看当前系统的 IP 地址，如下图所示：



可使用 Prev 和 Next 按纽进行翻页，Prev 是往前翻，Next 是往后翻；可用 Quit 退出 ps 命令行。使用左右键进行移动。

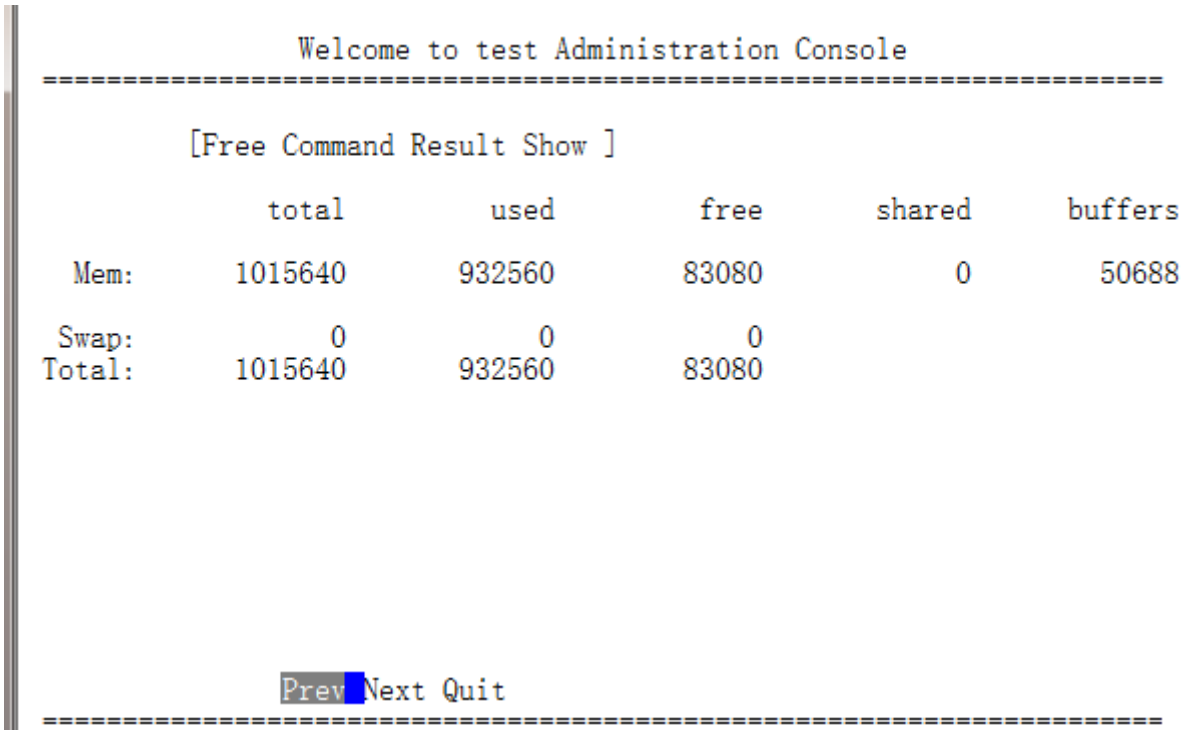
Netstat：查看当前系统的所有活跃端口。如下图所示：



可使用 Prev 和 Next 按纽进行翻页，Prev 是往前翻，Next 是往后翻；可用 Quit 退出 ps 命令行。使用

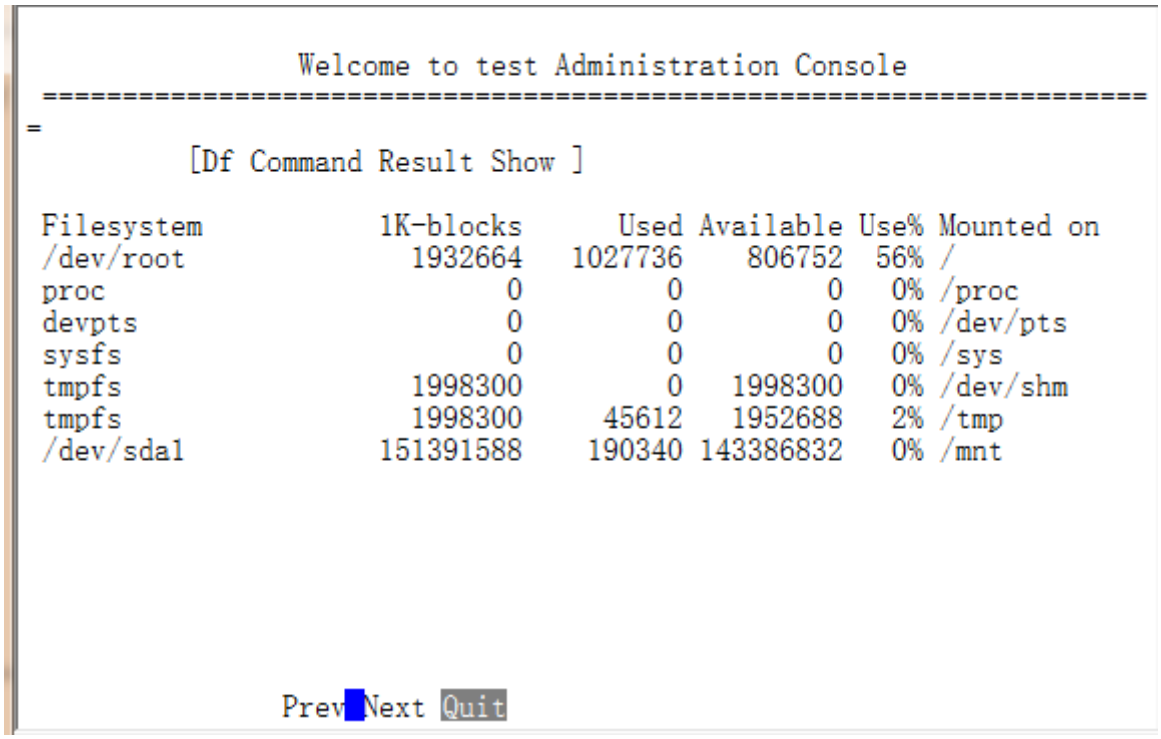
左右键进行移动。

Freememory：查看当前系统的内存信息。如下图所示：



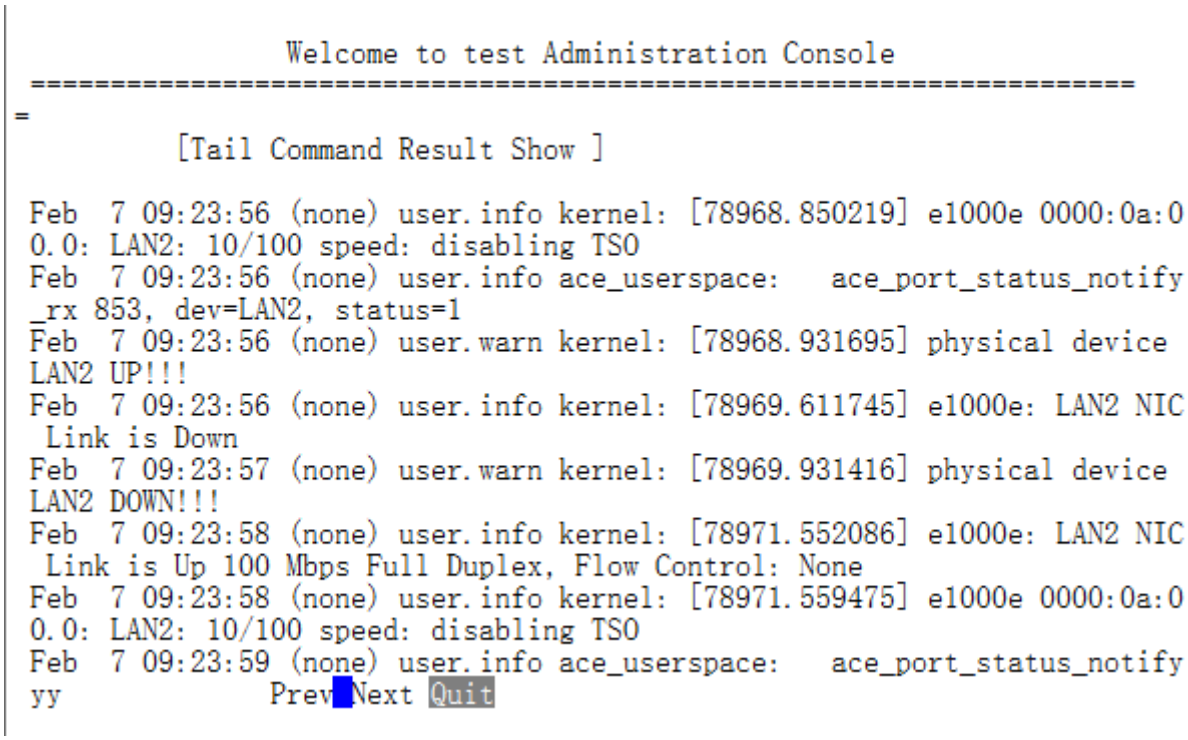
可使用 Prev 和 Next 按纽进行翻页，Prev 是往前翻，Next 是往后翻；可用 Quit 退出 ps 命令行。使用左右键进行移动。

Df：用来查看系统的磁盘空间占用情况。



可使用 Prev 和 Next 按纽进行翻页，Prev 是往前翻，Next 是往后翻；可用 Quit 退出 ps 命令行。使用左右键进行移动。

Syslog(100 line)：显示当前系统的最近 100 的日志信息。如下图所示：



可使用 Prev 和 Next 按纽进行翻页，Prev 是往前翻，Next 是往后翻；可用 Quit 退出 ps 命令行。使用左右键进行移动。

Syslog(all)：显示当前系统所有的日志信息。如下图所示：

```
                Welcome to test Administration Console
=========================================================================

          [Dmesg Command Result Show ]

000e 0000:0d:00.0: eth5: (PCI Express:2.5GT/s:Width x1) 00:0b:ab:57:b9:3
9
[    7.920826] e1000e 0000:0d:00.0: eth5: Intel(R) PRO/1000 Network Conn
ection
[    7.927857] e1000e 0000:0d:00.0: eth5: MAC: 4, PHY: 8, PBA No: FFFFFF
-0FF
[    7.934744] insmod used greatest stack depth: 6548 bytes left
[    8.049941] sshd used greatest stack depth: 6072 bytes left
[    8.098196] device LAN1 entered promiscuous mode
[    8.209603] e1000e 0000:08:00.0: irq 40 for MSI/MSI-X
[    8.267928] e1000e 0000:08:00.0: irq 40 for MSI/MSI-X
[    8.268632] ADDRCONF(NETDEV_UP): LAN1: link is not ready
[    8.308198] device WAN1 entered promiscuous mode
[    8.419530] e1000e 0000:09:00.0: irq 41 for MSI/MSI-X
[    8.477869] e1000e 0000:09:00.0: irq 41 for MSI/MSI-X
               Prev Next Quit
=========================================================================
```

可使用 Prev 和 Next 按纽进行翻页，Prev 是往前翻，Next 是往后翻；可用 Quit 退出 ps 命令行。使用左右键进行移动。

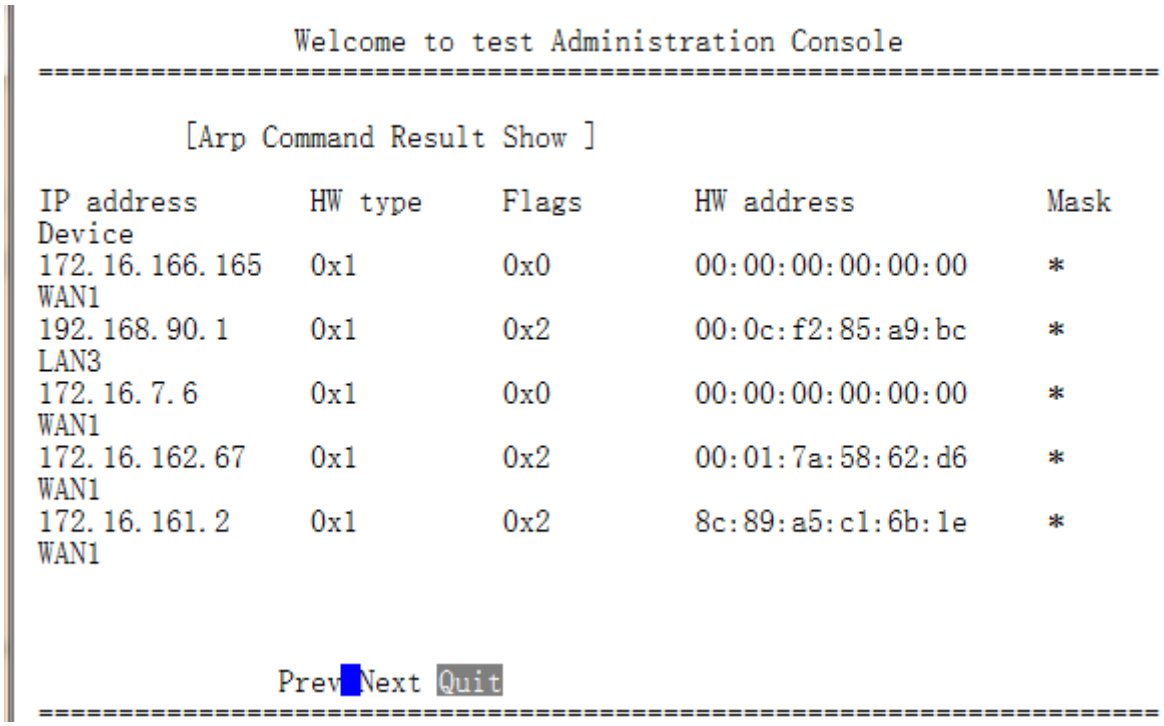
Route：查看系统的路由信息。如下图所示：

```
                Welcome to test Administration Console
=========================================================================

          [Route Command Result Show ]

default via 172.16.161.2 dev WAN1
172.16.0.0/16 dev WAN1  proto kernel  scope link  src 172.16.9.99
192.168.80.0/24 via 192.168.90.1 dev LAN3
192.168.90.0/24 dev LAN3  proto kernel  scope link  src 192.168.90.3
192.168.100.0/24 dev LAN1  proto kernel  scope link  src 192.168.100.1

192.168.200.0/24 dev LAN2  proto kernel  scope link  src 192.168.200.1









               Prev Next Quit
=========================================================================
```

可使用 Prev 和 Next 按纽进行翻页，Prev 是往前翻，Next 是往后翻；可用 Quit 退出 ps 命令行。使用

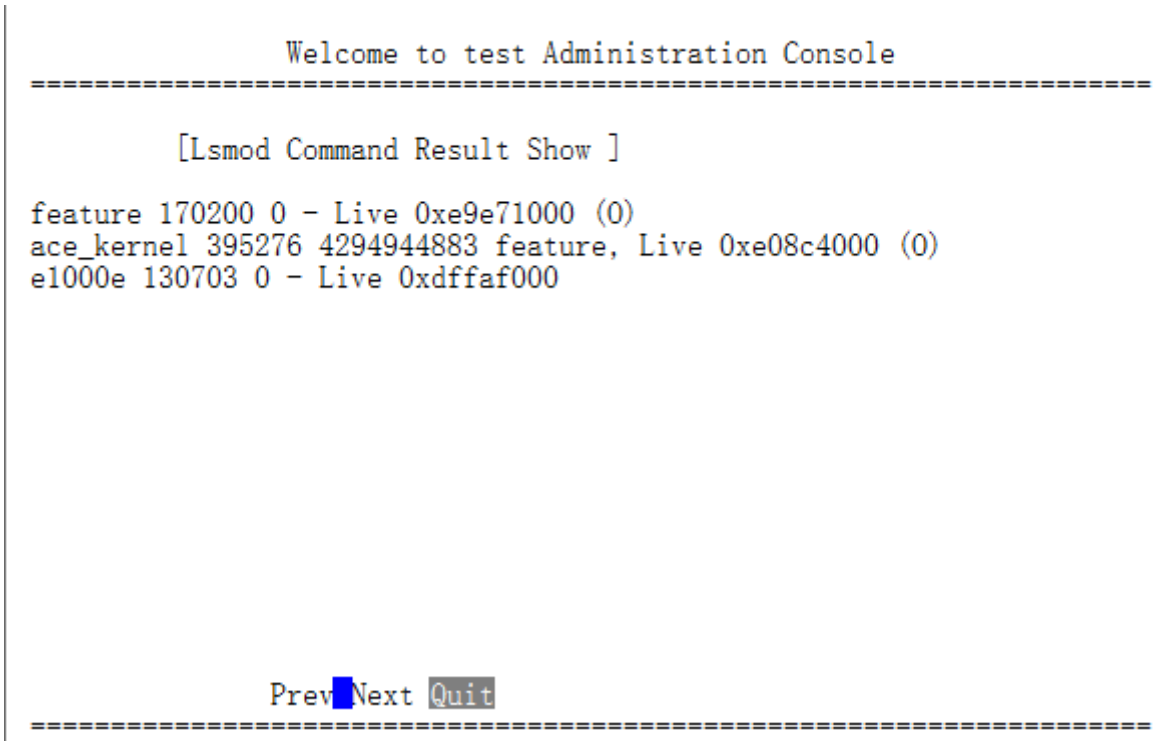
左右键进行移动。

Arp：查看系统的 arp 信息。如下图所示：



可使用 Prev 和 Next 按纽进行翻页，Prev 是往前翻，Next 是往后翻；可用 Quit 退出 ps 命令行。使用左右键进行移动。

Lsmod：列出所有已载入系统的模块。如下图所示：



Top：提供了实时的对系统处理器的状态监视。如下图所示：

```
                Welcome to test Administration Console
=============================================================================

         [Top Command Result Show ]

Mem: 933608K used, 82032K free, 0K shrd, 51336K buff, 532640K cached
CPU:  0.0% usr  0.0% sys  0.0% nic  100% idle  0.0% io  0.0% irq
0.0% sirq
Load average: 2.31 2.53 2.57 1/129 28484
  PID  STAT  %MEM  %CPU
  648     S  47.0   0.0
  322     S  26.2   0.0
  611    S<  17.1   0.0
  699     S  15.0   0.0
  621    S<  14.9   0.0
  670     S  11.6   0.0
  296     S  11.1   0.0
  753     S  11.0   0.0
  702     S  11.0   0.0
  695     S   4.8   0.0
              Prev Next Quit
=============================================================================
```

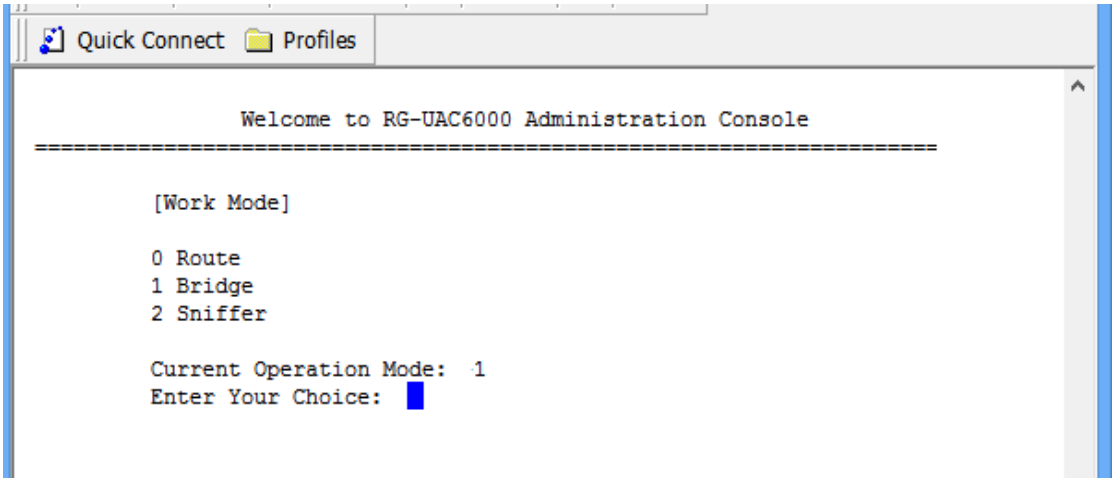
可使用 Prev 和 Next 按纽进行翻页，Prev 是往前翻，Next 是往后翻；可用 Quit 退出 ps 命令行。使用左右键进行移动。

1.3.2 查看系统的工作模式

后台一级密码登陆，选择菜单 Work Mode

```
                Welcome to test Administration Console
 ================================================================
=====
          [Main Menu]

          System Status
          Serial Number
          Version Information
          Work Mode
          Management IP Address
          System Update
          Download Debug information
          Add Route Table
          Reset Factory Default
          Save Configuration
          Reset WebUI Password & Management Policy
          Reboot
          Debug


 ================================================================
=====
```

按回车键



0 Route，表示路由模式；

1 Bridge，表示透明/桥模式；

2 Sniffer，表示旁路模式。ESC 键退出返回一级登录菜单。

1.3.3 查看系统版本以及特征库等信息

查看系统版本信息方法：登陆后台一级菜单，上下键选择 Version Information 菜单，按回车键

```
                Welcome to test Administration Console
================================================================================
====
          [Main Menu]

          System Status
          Serial Number
          Version Information
          Work Mode
          Management IP Address
          System Update
          Download Debug information
          Add Route Table
          Reset Factory Default
          Save Configuration
          Reset WebUI Password & Management Policy
          Reboot
          Debug
```

```
                Welcome to aa Administration Console
================================================================================

          Firmware:V1.0, build 141015.113009
          Feature:AIS-2.3.0.1, build 141010.161549
          URL:URL-2.3.0.1, build 141010.161557
          Client:IMS-1.7.16, build 141013.110114
          ISP:ISP-1.0.0.0, build 121012.185930









          Note:Press Enter To Return
================================================================================
Connected to 172.16.162.220   SSH2 - aes128-cbc - hmac-md5   80x24
```

再次回车键，返回后台一级密码登陆界面。

1.3.4 查看系统license信息

查看系统 license 信息方法：

登陆系统后台一级菜单，上下键选择菜单 Serial Number：

```
                Welcome to test Administration Console
 ================================================================
=====
          [Main Menu]

          System Status
          Serial Number
          Version Information
          Work Mode
          Management IP Address
          System Update
          Download Debug information
          Add Route Table
          Reset Factory Default
          Save Configuration
          Reset WebUI Password & Management Policy
          Reboot
          Debug
```

按回车键：

```
                Welcome to aa Administration Console
================================================================================

          Device Serial Number:
          84457d48da479b97b4b3b60e540bcb6d
          License Type:                   Demo
          License Status:                 Available
          License Issued date:            2014-10-13
          Demo Expired Date:              2015-01-11
          Firmware Update Expired Date:   2015-01-11
          Customer: 试用设备-RG-UAC6000
          Vendor: 锐捷
          WebUI Language:                 English+Simplified

          Authorized Session Number:      256K
          Authorized L7 Throughput:       100Mbps
          Authorized Firewall Throughput:100Mbps



          Note:Press Enter To Return
================================================================================
```

再次按回车键，返回后台一级密码登陆界面；或者 ESC 键返回一级密码登陆界面。

1.3.5 修改IP地址

修改 IP 地址有两种方法

1）登陆系统后台一级菜单，上下键选择菜单 Mangement Information：

```
                Welcome to test Administration Console
 ================================================================
=====
          [Main Menu]

          System Status
          Serial Number
          Version Information
          Work Mode
          Management IP Address
          System Update
          Download Debug information
          Add Route Table
          Reset Factory Default
          Save Configuration
          Reset WebUI Password & Management Policy
          Reboot
          Debug


 ================================================================
```

按回车键

```
                Welcome to test Administration Console
 ================================================================

          [Management IP Address]

          Ifname :  LAN1
          IP Address And Netmask:  172.16.4.221









          Note:Press Tab To Switch Port,Press Enter to Edit.
 ================================================================
```

按 Tab 键选择端口，按回车键对 IP 进行编辑。Esc 键返回一上级菜单。

2）选择一级菜单 Debug，按回车键，使用账号密码 admin/Login*PWD 进入命令行，执行 ifconfig 命令：

【参数说明】

参数	描述
	显示系统中所有接口信息
-a	显示系统中所有接口信息
Bridge1	显示 Bridge1（桥 1）接口信息
LAN1	显示 LAN1 接口信息

【配置举例】

查看设备 Bridge（桥 1）接口 ip

[HOSTNAME@root]ifconfig Bridge1

配置接口 IP

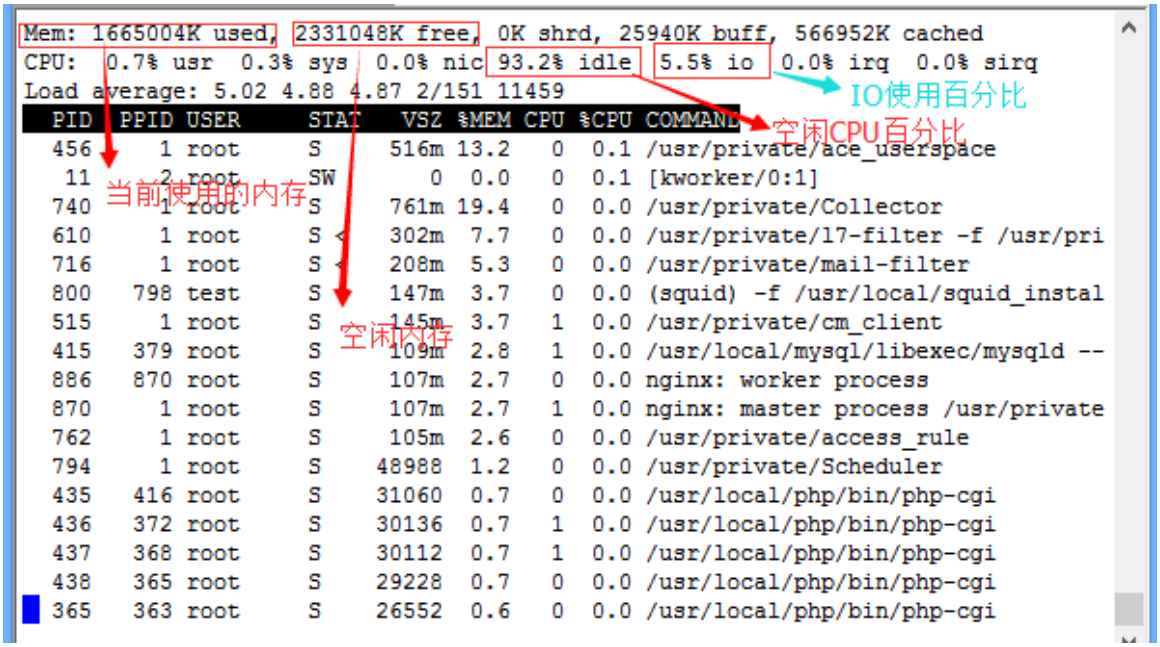
[HOSTNAME@root]ifconfig Bridge1 192.168.0.1/24

清除接口 IP

[HOSTNAME@root]ifconfig Bridge1 0

1.3.6 查看系统运行CPU、内存使用情况

1. debug 登陆后台，命令行执行 top，Ctrl +C 退出。



1.3.7 route命令

查看设备路由，请执行 route 命令：

【参数说明】

参数	描述
	显示和操作 IP 路由表
-n	显示路由表
add	添加静态路由
del	删除静态路由

【配置举例】

查看设备路由表

[HOSTNAME@root]route

[HOSTNAME@root]route–n

添加到目的主机路由：

[HOSTNAME@root]route add 192.168.10.2 gw 192.168.1.1

添加到目标主机路由：

[HOSTNAME@root]route add -net 192.168.10.0 netmask 255.255.255.0 gw

192.168.1.1

添加缺省静态路由：

[HOSTNAME@root]route add default gw 172.16.161.2

删除到目的主机路由：

[HOSTNAME@root]route del 192.168.10.2 gw 192.168.1.1

删除到目标主机路由：

[HOSTNAME@root]route del -net 192.168.10.0 netmask 255.255.255.0 gw 192.168.1.1

删除缺省静态路由：

[HOSTNAME@root]route del default gw 172.16.161.2

1.3.8 ping 命令

ping 命令用来测试与目标主机连通性

【参数说明】

参数	描述
	测试与目标主机连通性，默认一直 ping，CRL+C 退出 ping
-c	指定 ping 次数
-s	指定 ping 报文字节数
-I	指定 ping 的网络界面送出数据包

【配置举例】

[HOSTNAME@root]ping 172.16.161.2 -c 2

PING 172.16.161.2 (172.16.161.2): 56 data bytes

64 bytes from 172.16.161.2: seq=0 ttl=64 time=2.127 ms

64 bytes from 172.16.161.2: seq=1 ttl=64 time=2.174 ms

--- 172.16.161.2 ping statistics ---

2 packets transmitted, 2 packets received, 0% packet loss

round-trip min/avg/max = 2.127/2.150/2.174 ms

[HOSTNAME@root]ping 172.16.161.2 -s 1000 -c 2

PING 172.16.161.2 (172.16.161.2): 1000 data bytes

1008 bytes from 172.16.161.2: seq=0 ttl=64 time=2.886 ms

1008 bytes from 172.16.161.2: seq=1 ttl=64 time=2.823 ms

--- 172.16.161.2 ping statistics ---

2 packets transmitted, 2 packets received, 0% packet loss

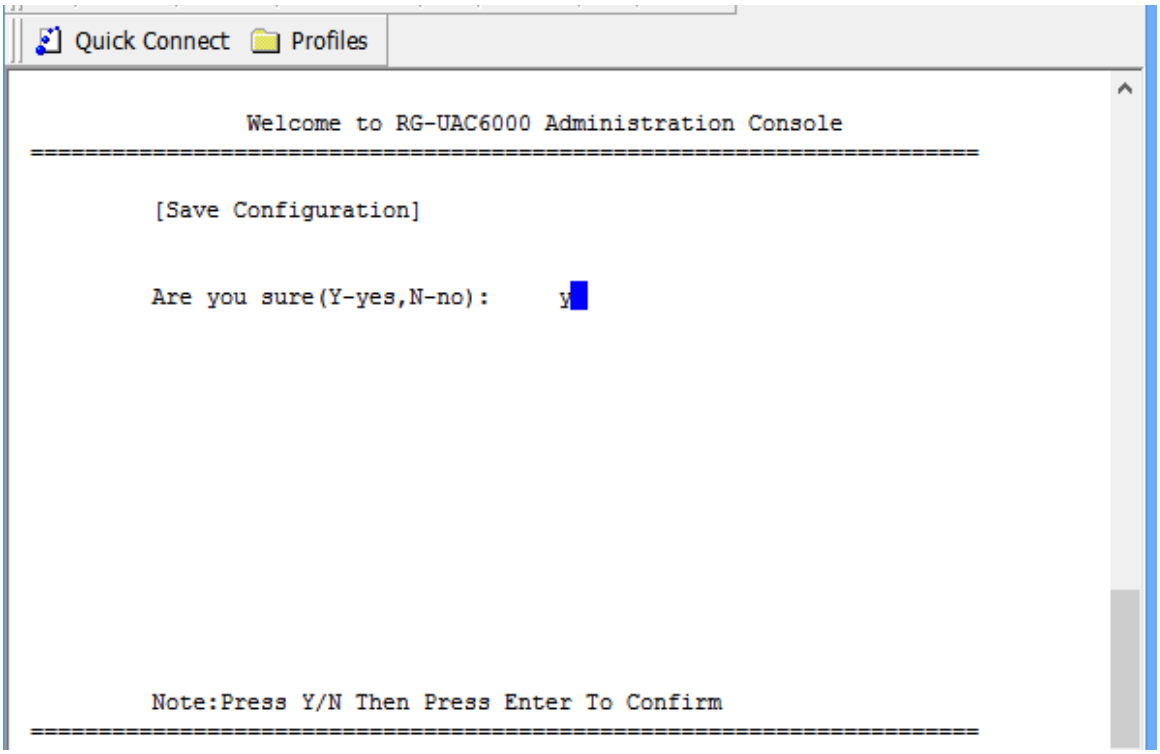
round-trip min/avg/max = 2.823/2.854/2.886 ms

1.3.9 配置保存

1. 后台一级密码登陆，选择菜单 Save Configuration。

```
                Welcome to test Administration Console
================================================================================
====
          [Main Menu]

          System Status
          Serial Number
          Version Information
          Work Mode
          Management IP Address
          System Update
          Download Debug information
          Add Route Table
          Reset Factory Default
          Save Configuration
          Reset WebUI Password & Management Policy
          Reboot
          Debug



================================================================================
----
```

按回车键，选择 y，表示确认保存配置，n 表示不保存；

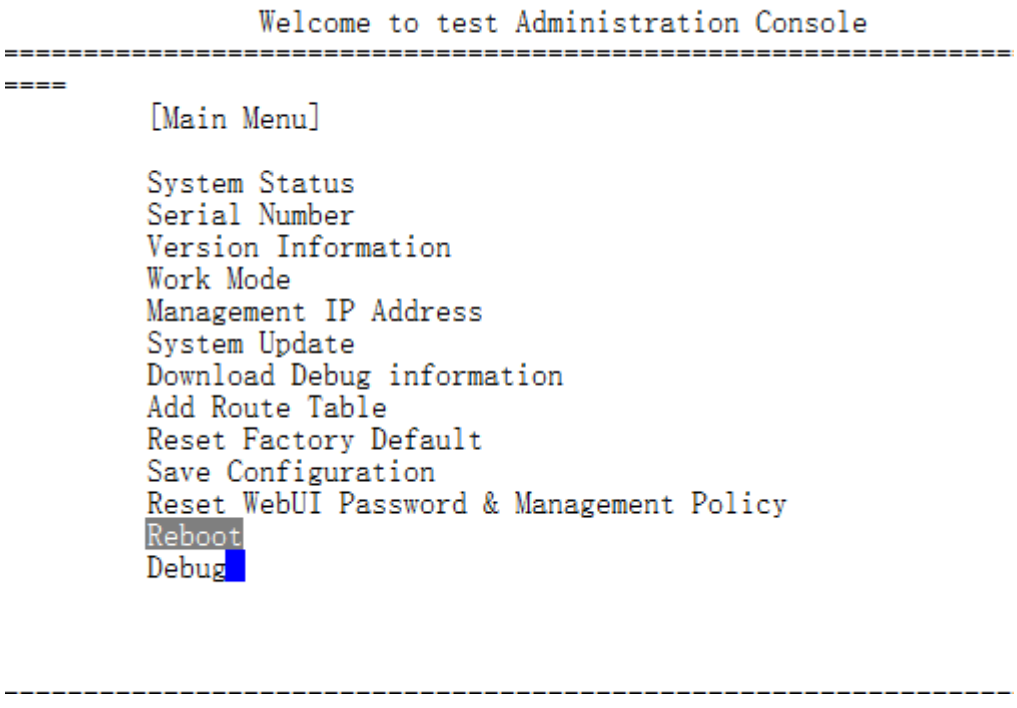


2. 在 web 管理界面点击保存按钮，save 当前配置信息

1.3.10 reboot 命令

reboot 用来重启系统，谨慎操作，重启前，请确认是否需要保存配置。

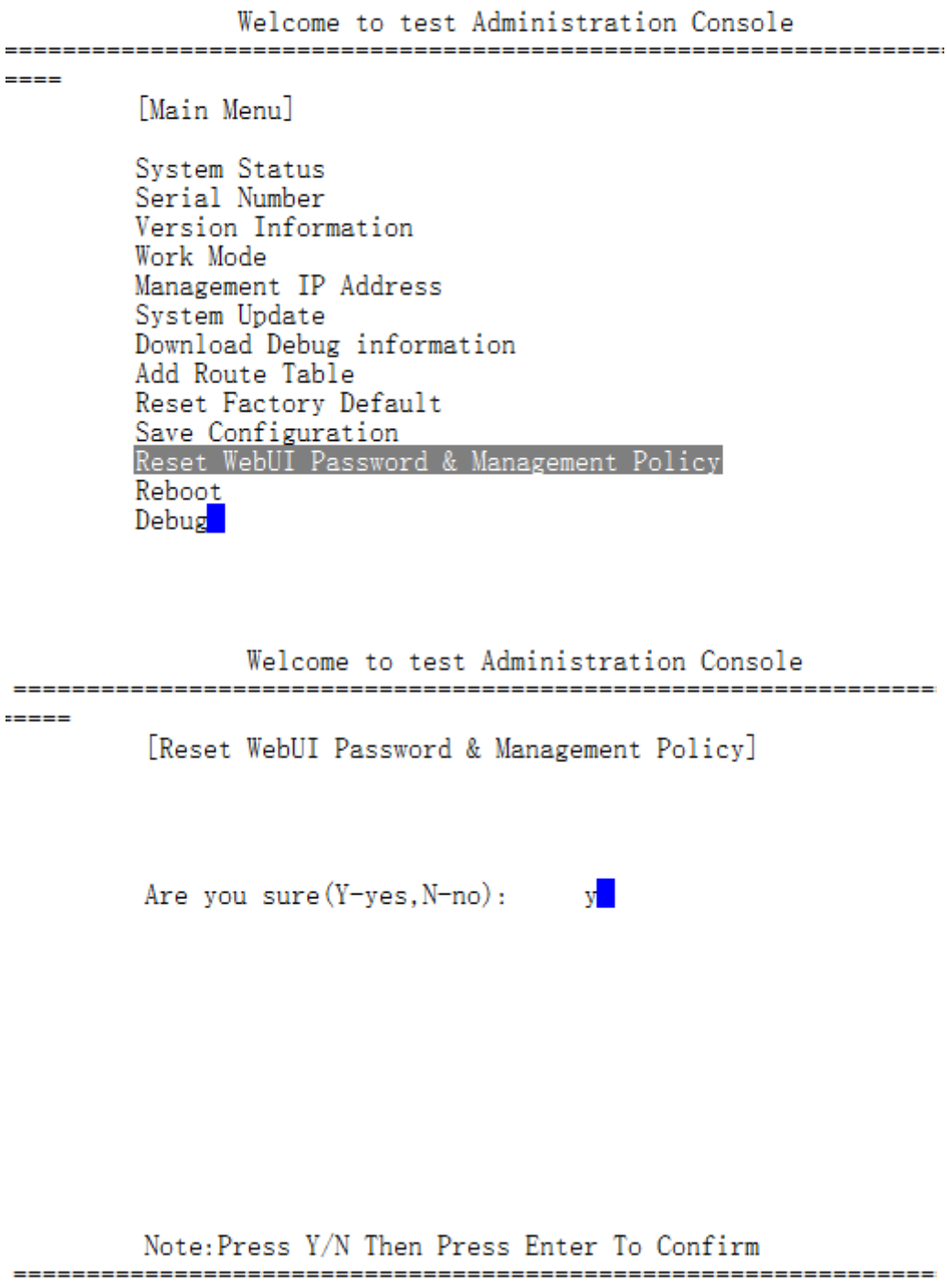
1. 一级密码登陆后台，上下键选择菜单 Reboot ，回车。



2. Debug 登录系统，命令行执行 reboot，回车

1.3.11 恢复web管理界面密码及网管策略

1. 一级密码登陆后台，上下键选择到菜单：Reset WebUI Password，并回车



2. 如果是只需恢复 web 密码，还有另一种方法恢复：登陆 debug 菜单，执行一下操作

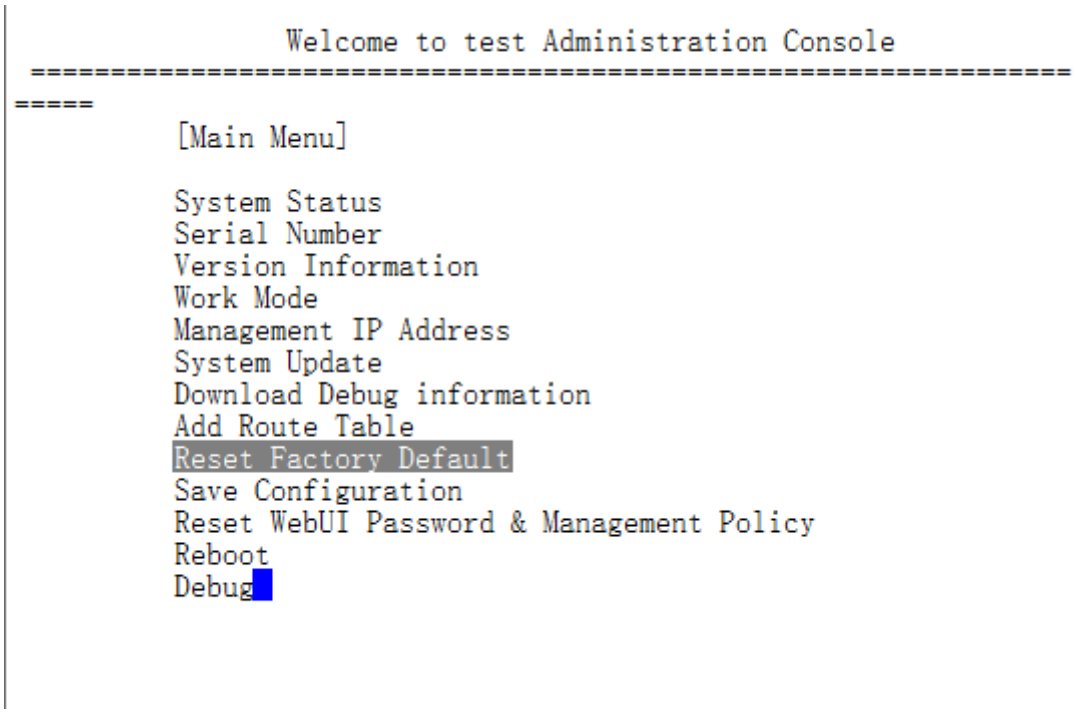
[HOSTNAME@root]cp /home/config/default/user.conf /usr/local/lighttpd/

[HOSTNAME@root]cp /home/config/default/user.conf /home/config/current

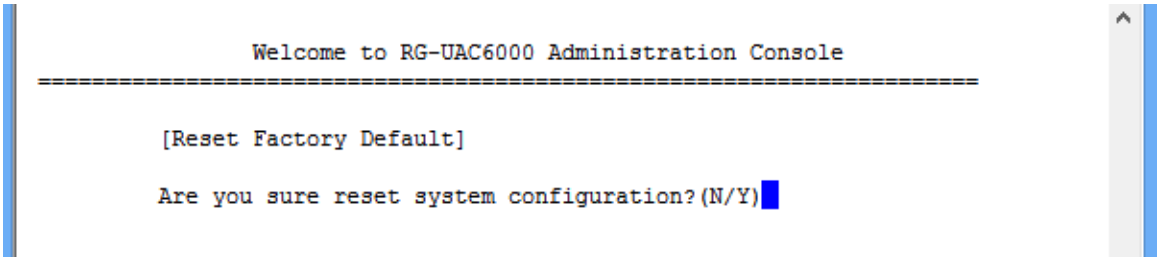
[HOSTNAME@root] service lighttpd restart

1.3.12 恢复出厂设置

1. 一级密码登陆后台，上下键选择菜单 Reset Factory Default，回车。



2. 选择 Y，表示确认恢复出厂设置，选择 N 表示退出设置。



1.3.13 Web管理界面超出最大登陆次数

Web 管理界面连续 5 次输错管理员密码，第 6 次输入用户名密码提示:登陆次数已达上限。登陆管理界面 IP+对应管理员账号，默认惩罚时间为 10 分钟，10 分钟后解除。

快速解除办法：

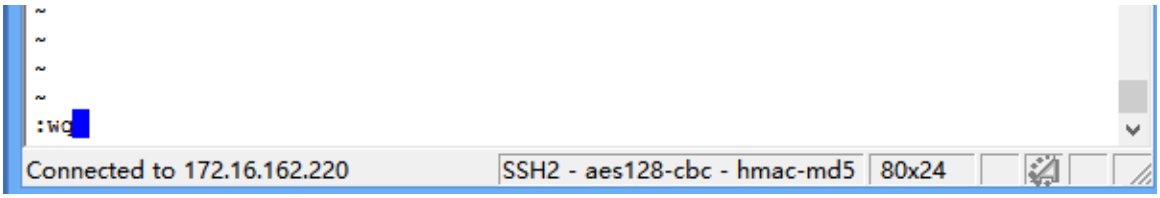
1. 修改 PC IP 登陆。

2. 登陆后台解除惩罚命令。

[HOSTNAME@root]vi /usr/local/lighttpd/webuser.conf

连续两次敲 dd，删除惩罚命令

然后 ESC 键，英文字符:wq 保存并退出



1.3.14 Web方式升级系统版本步骤

1、登陆webUI，进入**系统配置>系统维护>系统升级**，界面如下图所示。

(1)在“系统版本”处，单击“浏览”按钮，选择本地PC机上的升级文件包(升级包前缀命名为NACFirmware，后缀名为.bin，如NACFirmware_1.6.6_141021.195436_ruijie_0.bin，一般用下载时的升级文件名字即可，不需修改）。

(2)点击“确定”按扭提交设置后，升级文件开始上传到设备上，上传成功后，系统版本升级需要重启设备才能生效，重启会造成断网，合理选择重启时间，**请避开业务高峰期重启设备。**

2、重启完毕后，再次登陆WebUI，进入系统配置>系统维护>系统升级菜单可查看当前运行使用的版本信息：

1.3.15 命令方式升级系统版本步骤

命令行升级系统有两种方法

第一种方法：

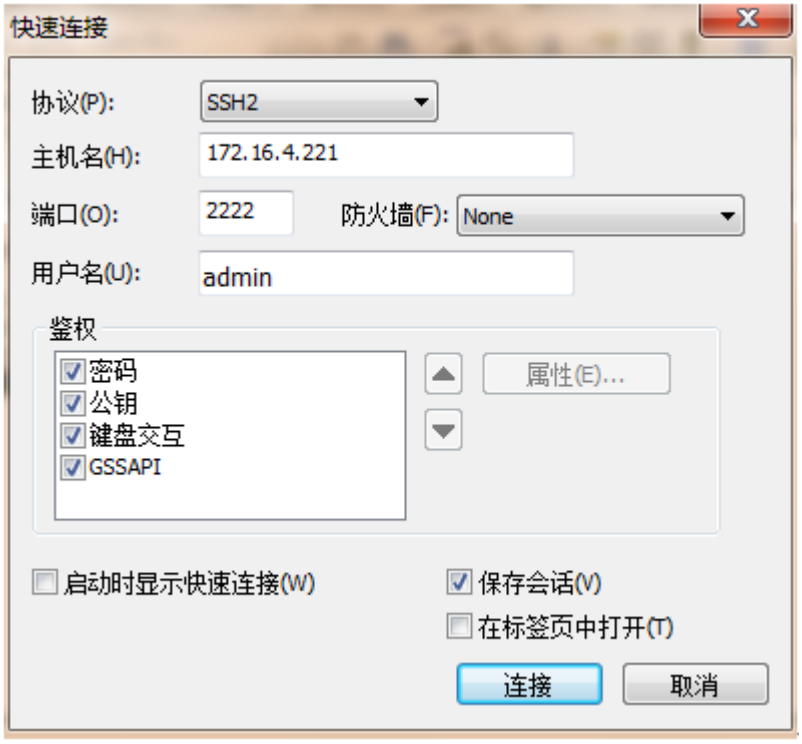
securecrt.zip

1、将特征库放在本地文件夹，安装

2、SSH方式登陆设备，需同时保证升级服务器与设备管理接口路由可达，否则无法上传升级文件；

双击 SecureCrt，登录方式：协议号选择 SSH2,主机名为设备实际管理 IP，端口：2222，用户名：root,

其他参数默认，填写完毕点击连接按钮。



3、 弹出输入密码框，admin对应默认密码为firewall**（注：如果web页面的admin用户密码修改，则会跟着修改该后台密码）**

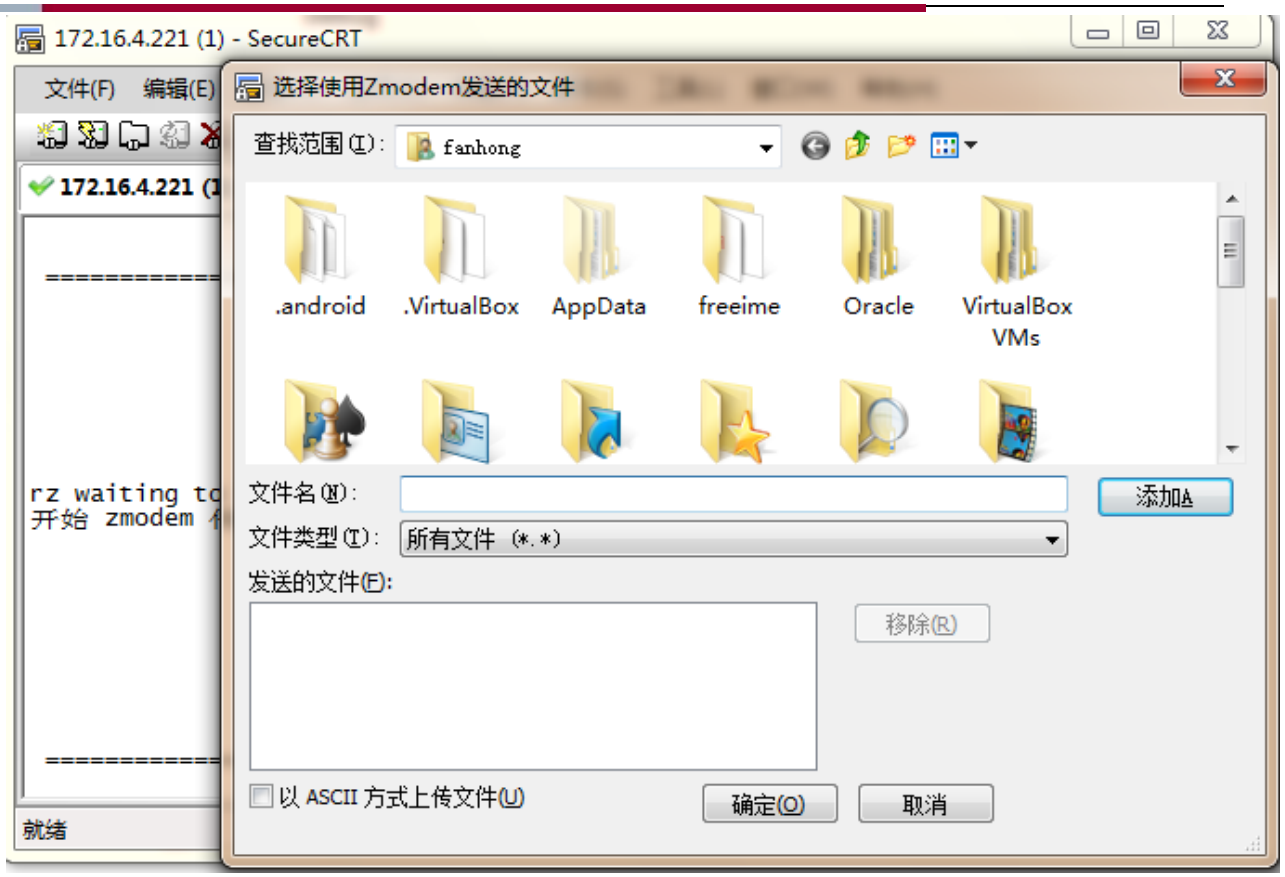
按上下键选择System Update

```
                Welcome to test Administration Console
 ================================================================
=====
          [Main Menu]

          System Status
          Serial Number
          Version Information
          Work Mode
          Management IP Address
          System Update
          Download Debug information
          Add Route Table
          Reset Factory Default
          Save Configuration
          Reset WebUI Password & Management Policy
          Reboot
          Debug


 ================================================================
=====
```

按回车键

```
                Welcome to test Administration Console
 ================================================================

          [System Update]

          System Firmware
          AIS Database
          URL Database
          Unit License
          Back









 ================================================================
```

选择System Firmware，按回车键



本地选中UAC6000系统升级包，点击添加，添加完成后点击确定。弹出如下界面：

```
rz waiting to receive.
开始 zmodem 传输。   按 Ctrl+C 取消。
   66%   34888 KB 8722 KB/s 00:00:02 ETA   0 Errorss507_ruijie_0.bin...



                        Note: Uploading ...
================================================================================
```

上传完成后，按Esc返回一级菜单。

UAC6000升级完成不会自动重启，需要重启设备才能生效，重启会造成断网，合理选择重启时间，**请避开业务高峰期。**

第二种方法：

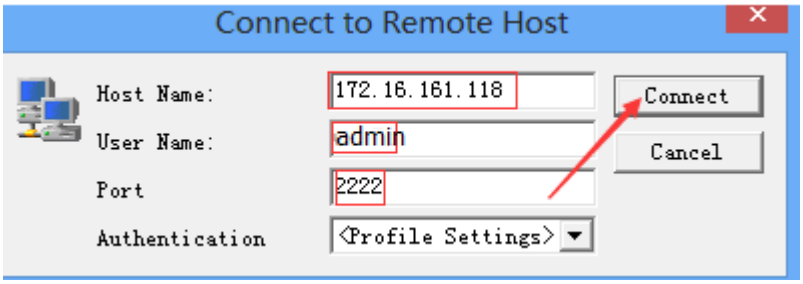
1、NACFirmware_1.6.6_141021.195436_ruijie_0.bin放在本地文件夹，安装

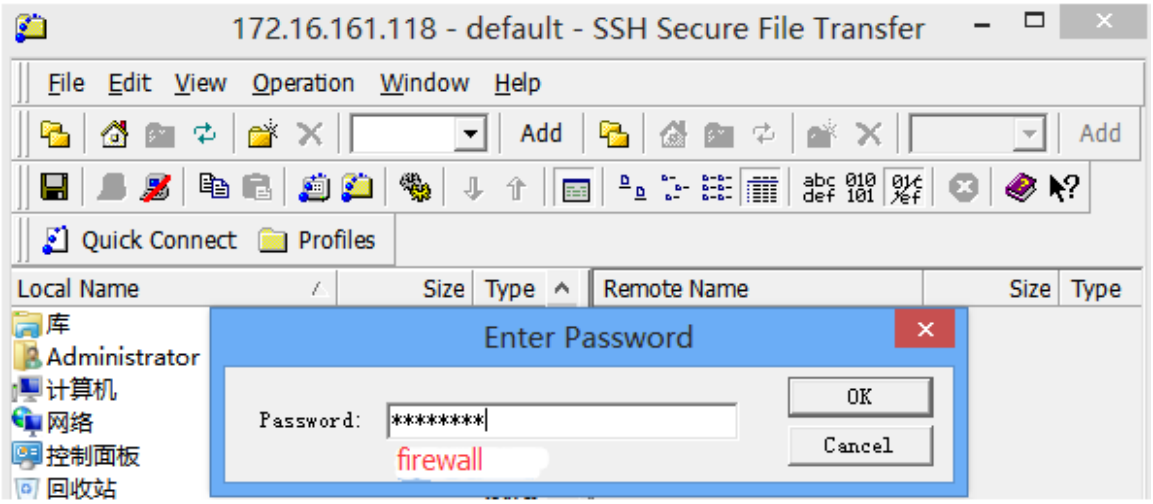
SSHSecureShellClient-3.2.9.exe

安装完成会有两个图标，一个用于命令行登录（左），一个用于文件传输（右）。

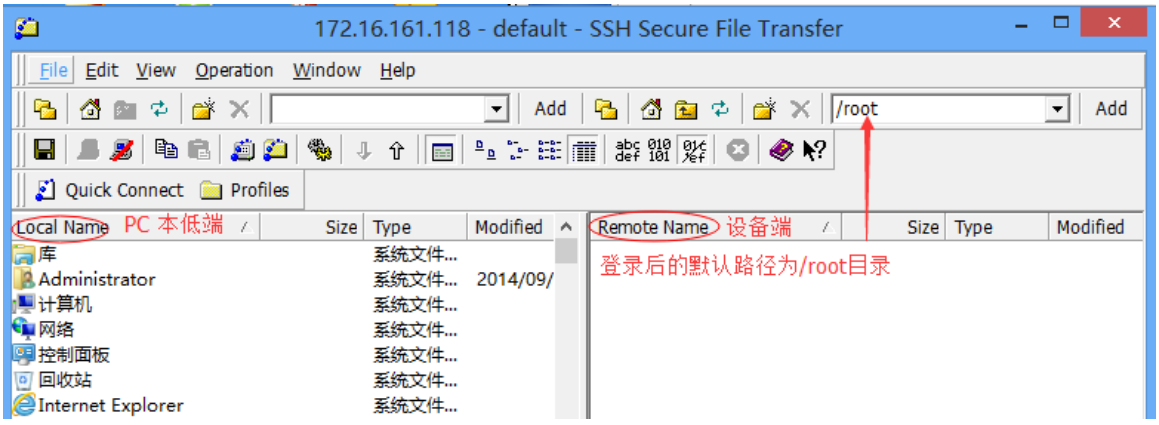
2、SSH方式登陆设备，需同时保证升级服务器与设备管理接口路由可达，否则无法上传升级文件；

双击SSH Secure File Transfer Client ,登录方式 :登录Host name 为设备**实际管理IP** ,User Name：admin，Port：2222，其他参数默认，填写完毕点击connect 按钮。



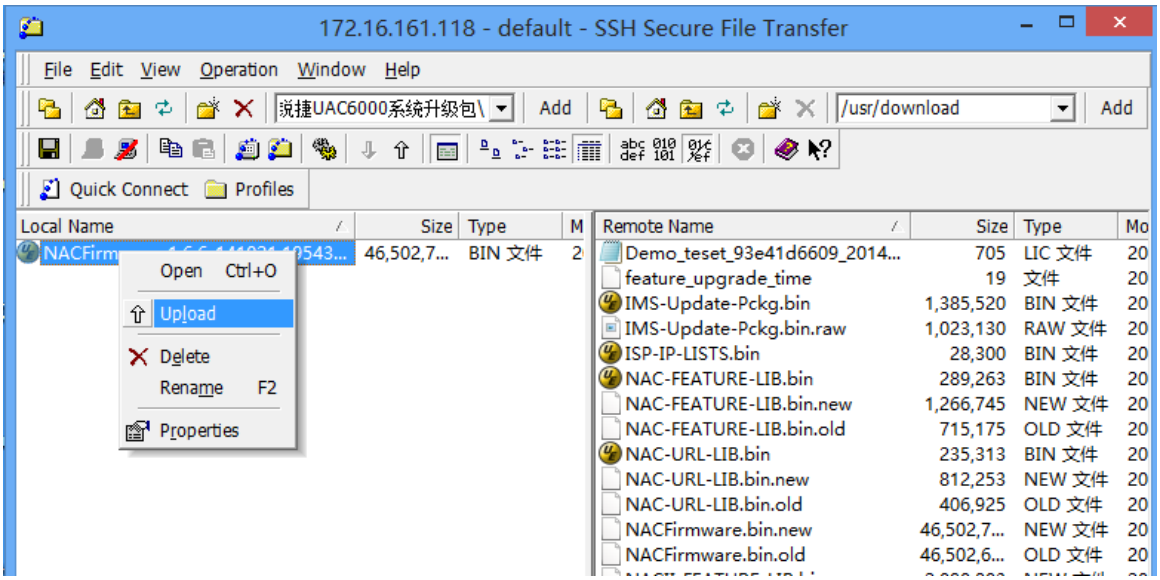


4、登录完成默认进到UAC6000 后台的/root目录：



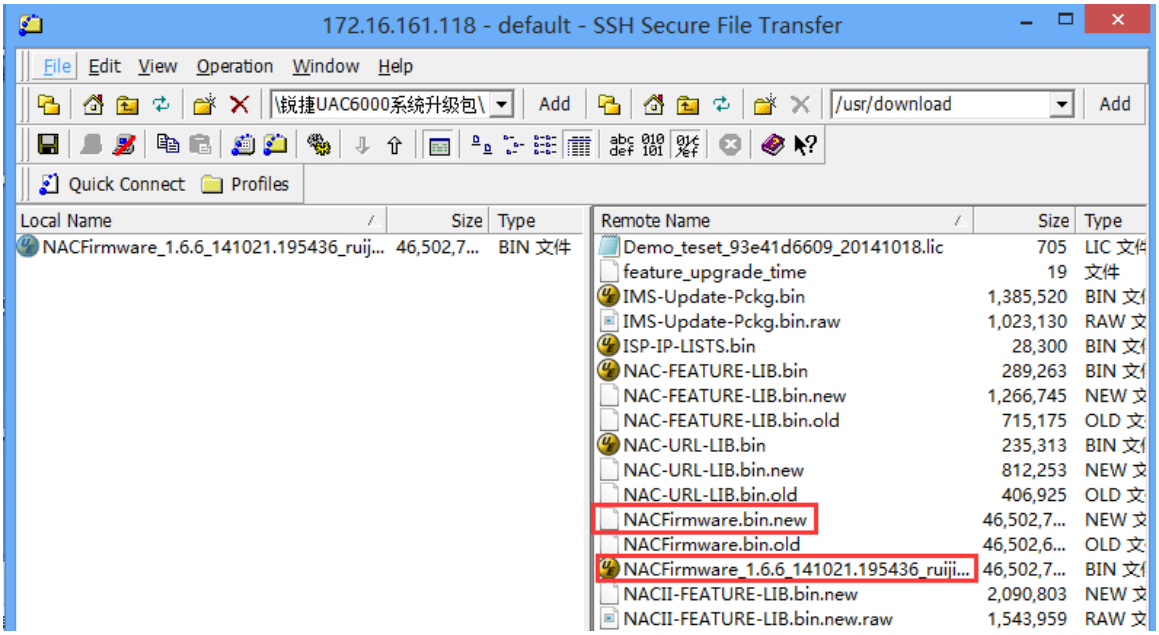
5、将本地升级文件包上传到设备/usr/download文件夹下：

本地选中UAC6000系统升级包，鼠标右键，选择Upload，上传；也可直接把系统升级包拖到右边文件框。

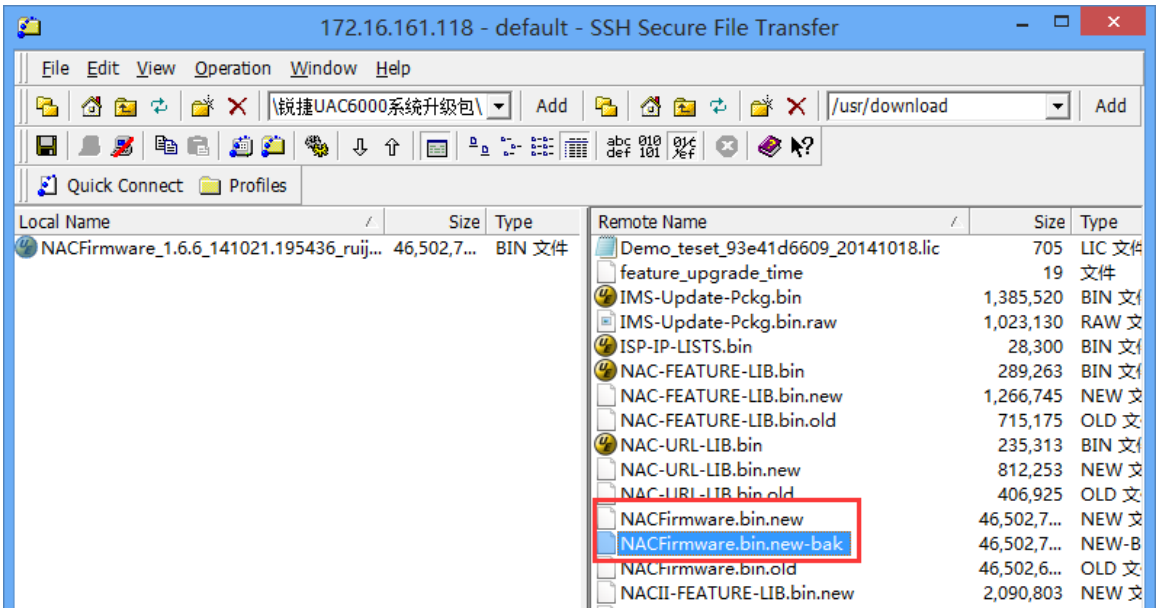


6、备份NACFirmware.bin.new，即修改NACFirmware.bin.new文件名字为NACFirmware.bin.new-bak；

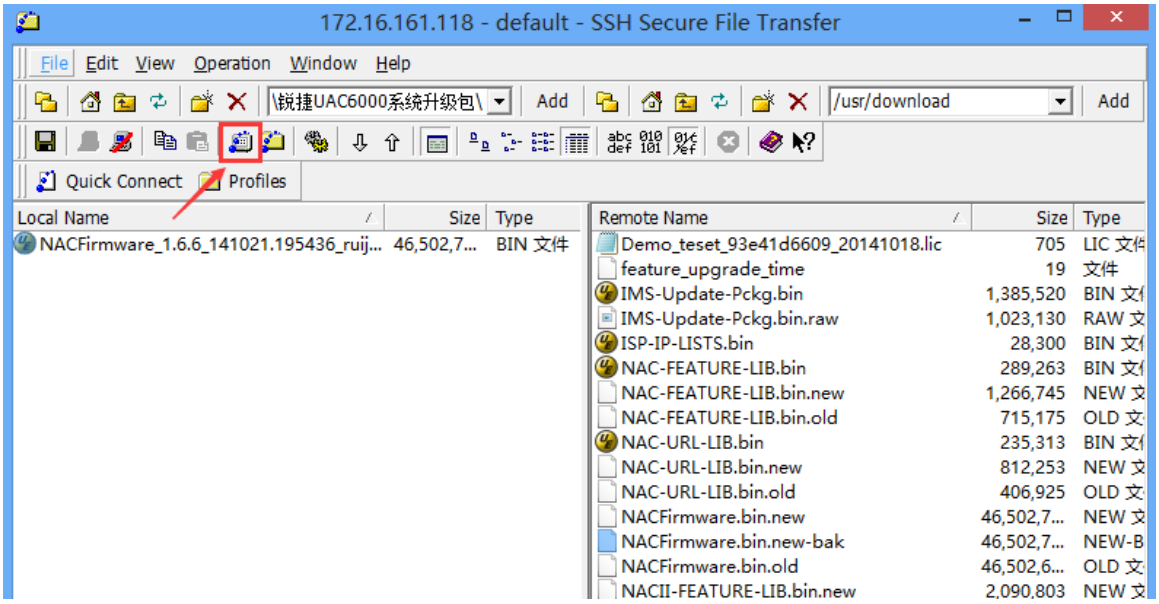
NACFirmware_1.6.6_141021.195436_ruijie_0.bin名称改为NACFirmware.bin.new



修改文件名称之后，如下：



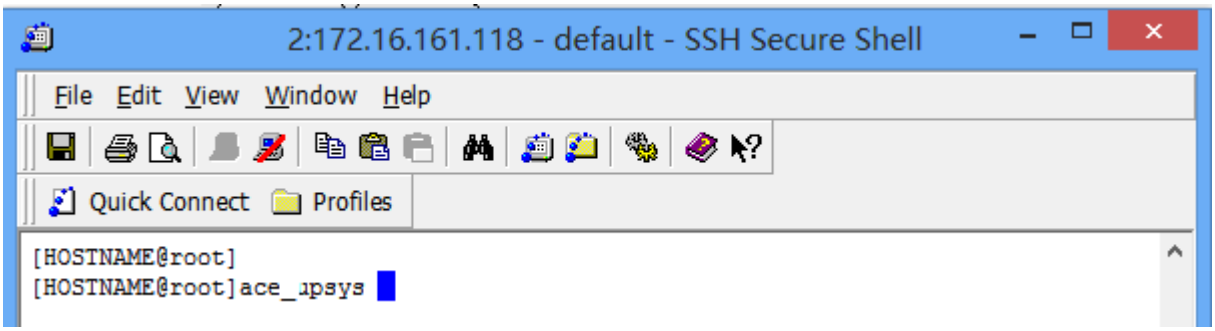
7、ssh登录命令行，选择如下图标：



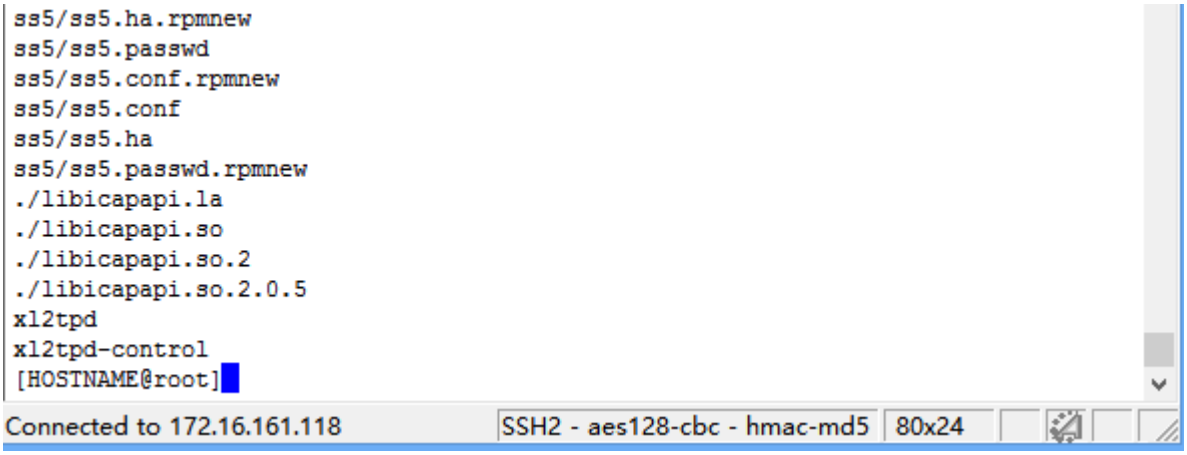
弹出窗口，上下键选择Debug菜单，回车,

```
                Welcome to test Administration Console
 ================================================================
=====
          [Main Menu]

          System Status
          Serial Number
          Version Information
          Work Mode
          Management IP Address
          System Update
          Download Debug information
          Add Route Table
          Reset Factory Default
          Save Configuration
          Reset WebUI Password & Management Policy
          Reboot
          Debug

  Username:admin      Password: *********  Login*PWD
 ================================================================
-----
```

8、命令行执行ace_upsys，回车，等待时间约一分钟，系统版本执行更新，界面会有更新日志打印

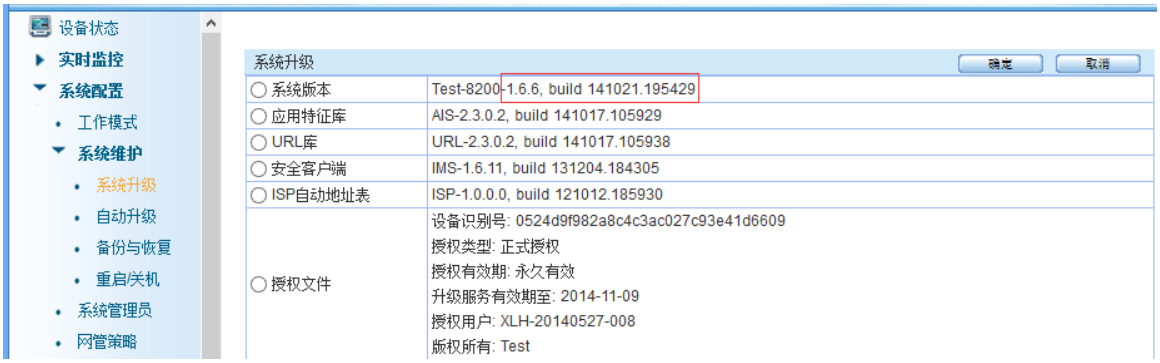


更新日志举例：



更新完成会到命令行，UAC6000升级完成不会自动重启，需要重启设备才能生效，重启会造成断网，合理选择重启时间，**请避开业务高峰期重启设备。**

9、重启完毕后，再次登陆WebUI，进入系统配置>系统维护>系统升级菜单可查看当前运行使用的版本信息：

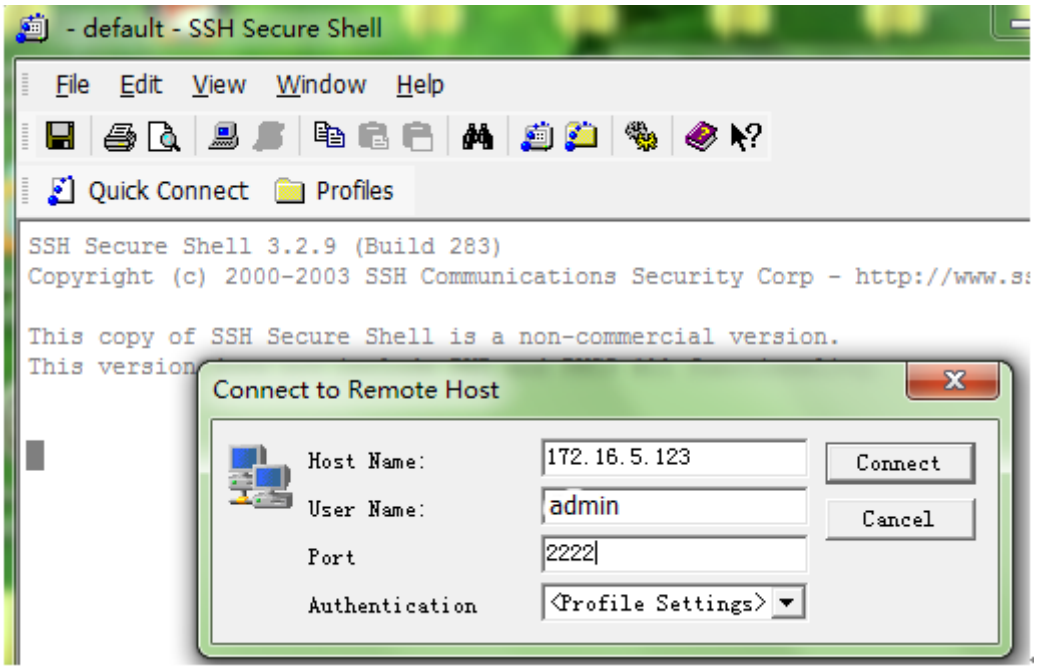


至此升级操作完成。

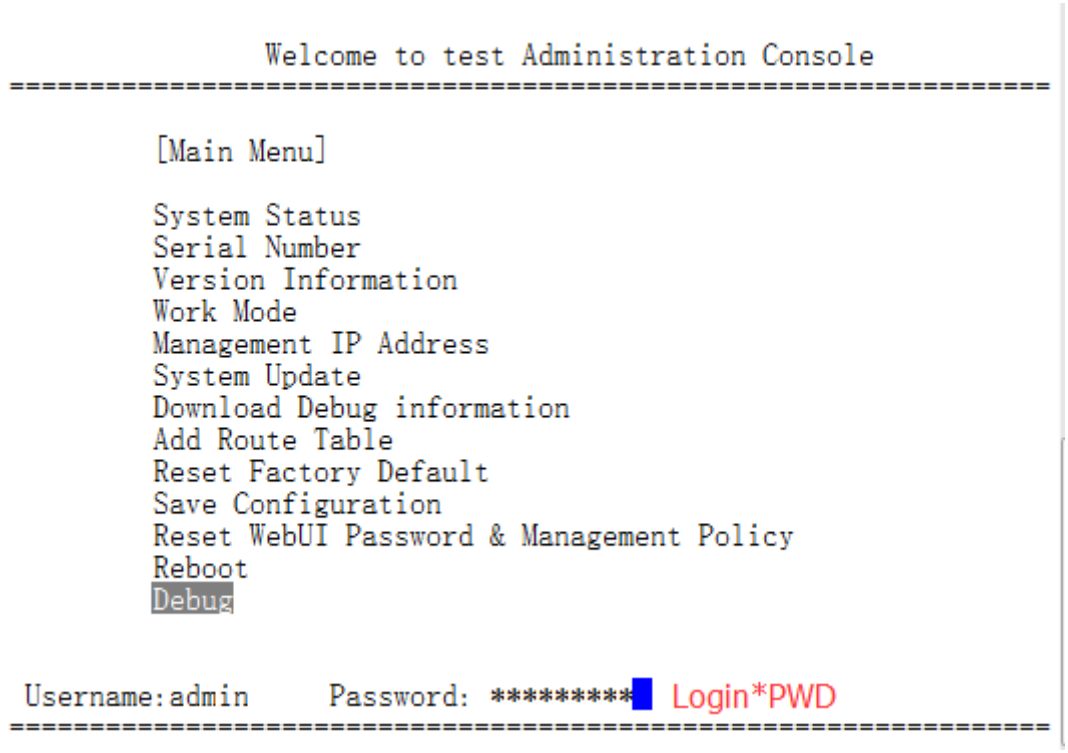
1.3.16 行为管理版本降级说明

1. 后台 SSH 登录

用户名 admin 默认密码 firewall（注：如果 web 页面的 admin 用户密码修改，则会跟着修改该后台密码） port: tcp 2222



二级用户名/密码：admin/Login*PWD

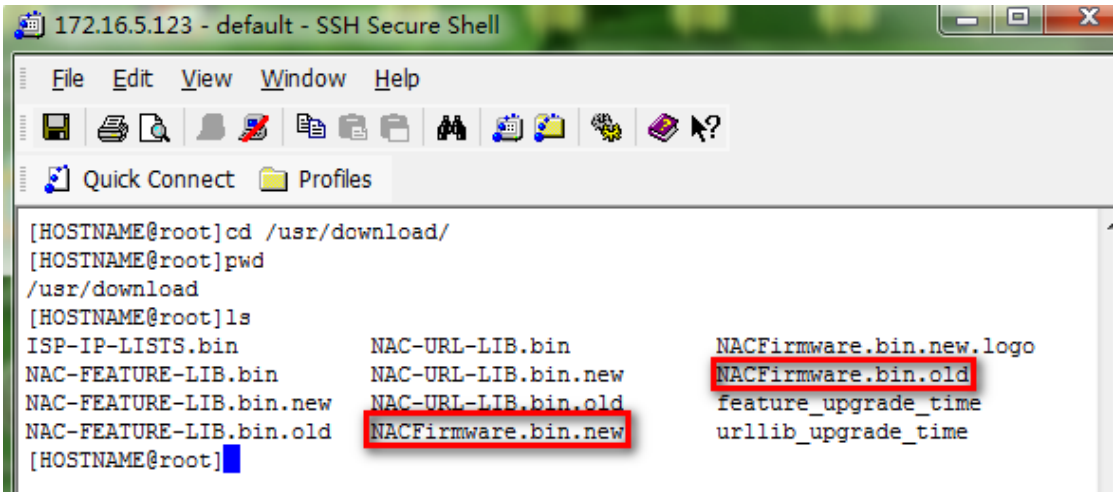


2. 到固件存储的路径

cd /usr/download

NACFirmware.bin.new 这个文件是当前生效的固件

NACFirmware.bin.old　　这是上一次升级的固件（备份用）



版本降级，需要

NACFirmware.bin.new　　重命名为 NACFirmware.bin.new1

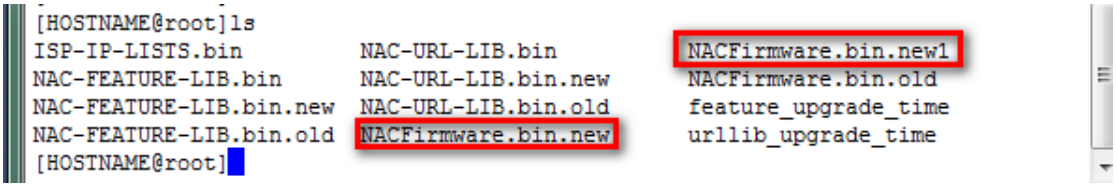
NACFirmware.bin.old 重命名为 NACFirmware.bin.new

命令分别为

[HOSTNAME@root]mv　NACFirmware.bin.new　NACFirmware.bin.new1

[HOSTNAME@root]mv　NACFirmware.bin.old NACFirmware.bin.new

查看一下



[HOSTNAME@root]cd　/root

[HOSTNAME@root]ace_upsys （执行系统更新命令）之后会有一些打印，这是正常，安装 spuid 而已

[HOSTNAME@root]exit （退出）

[HOSTNAME@root]reboot（重启设备，固件升级需要重启设备，才能生效）

1.3.17 命令方式升级URL库、特征库、授权文件步骤

升级特征库、URL库、授权文件的方法一样，此处只列出升级特征库的方法。

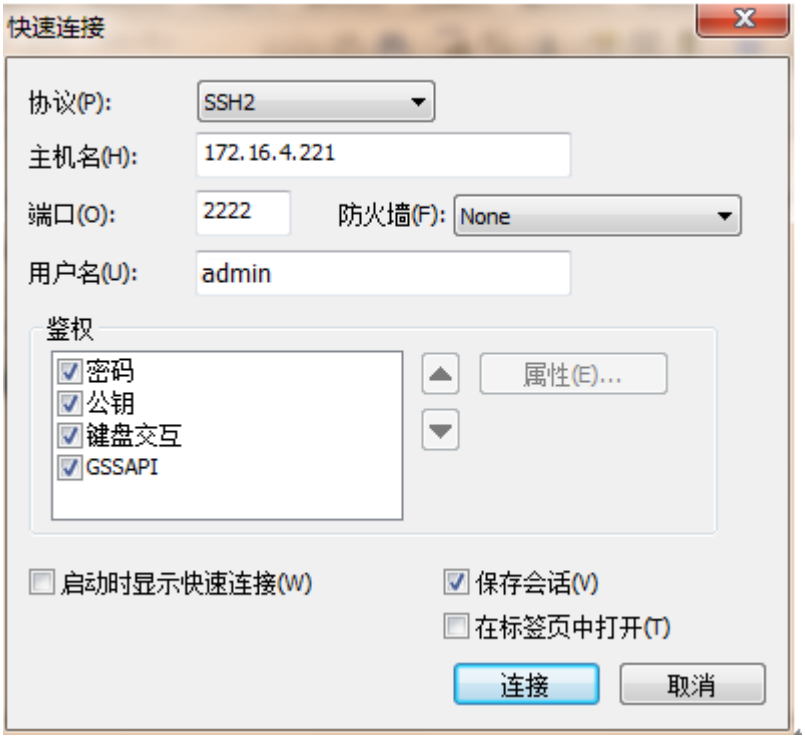

securecrt.zip

1、 将特征库放在本地文件夹，安装

2、SSH方式登陆设备，需同时保证升级服务器与设备管理接口路由可达，否则无法上传升级文件；

双击 SecureCrt ,登录方式 :协议号选择 SSH2,主机名为设备实际管理 IP ,端口 :2222 ,用户名 :admin,

其他参数默认，填写完毕点击连接按钮。



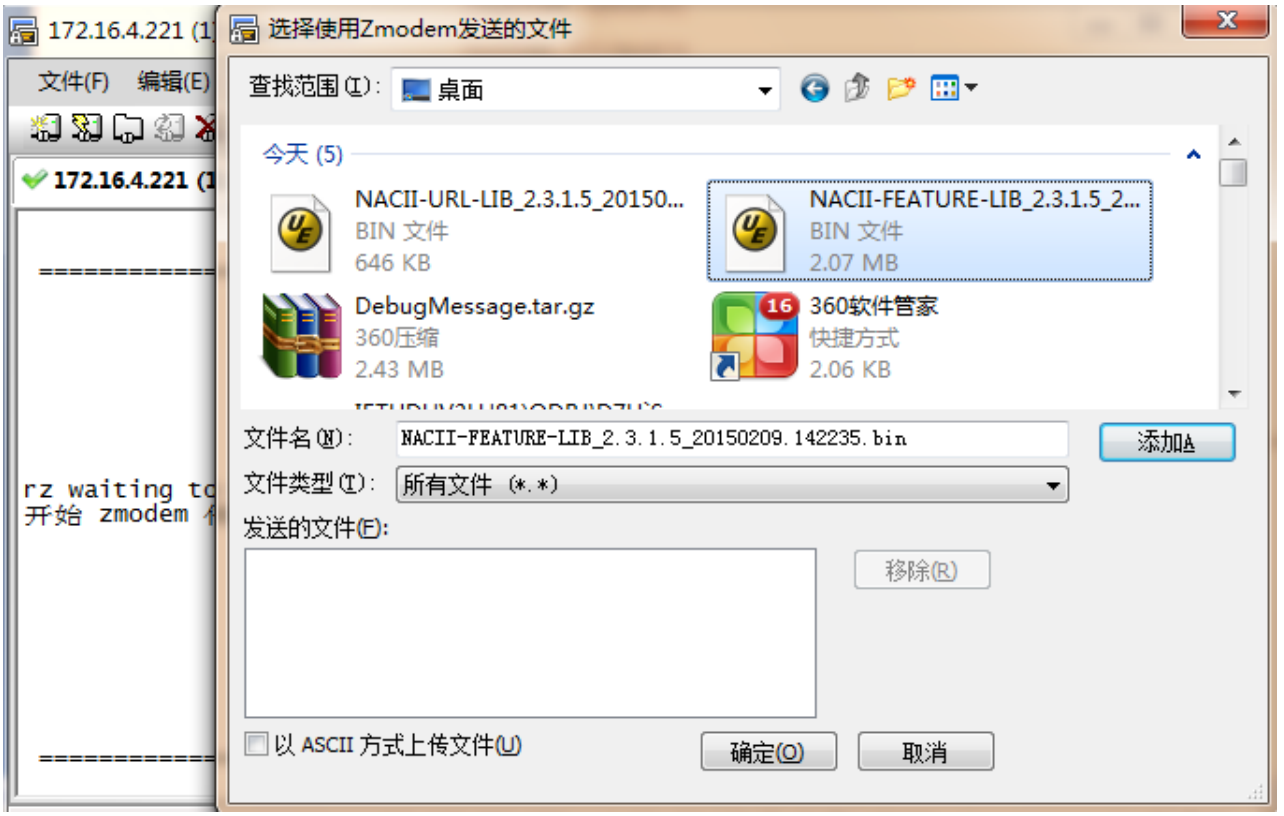
2、 弹出输入密码框，admin对应默认密码为firewall**（注：如果web页面的admin用户密码修改，则会跟着修改该后台密码）**按上下键选择System Update

```
                Welcome to test Administration Console
 ================================================================
=====
          [Main Menu]

          System Status
          Serial Number
          Version Information
          Work Mode
          Management IP Address
          System Update
          Download Debug information
          Add Route Table
          Reset Factory Default
          Save Configuration
          Reset WebUI Password & Management Policy
          Reboot
          Debug
```

按回车键

```
                    Welcome to test Administration Console
 ================================================================================

          [System Update]

          System Firmware
          AIS Database
          URL Database
          Unit License
          Back




 ================================================================================
```

选择AIS Database，按回车键



添加要上传的特征库，点击确定

```
                Welcome to test Administration Console
================================================================================
                          System Upgrade



rz waiting to receive.
开始 zmodem 传输。   按 Ctrl+C 取消。
  100%    2126 KB 2126 KB/s 00:00:01       0 Errors235.bin...


                        Note: seccessed.(Press [Esc] to exit)
================================================================================
```

等待完成即可。即时生效，不需要重启设备。

2 UAC 后台日志查询

2.1 配置日志功能

默认情况下，所有日志功能都是开启的，发向本地硬盘日志数据库。相关信息可以通过 WEB 页面查看。

2.2 查看系统进程运行状态日志信息

用于监控进程对应后台的进程的都在 sysappmonitor 日志；

查看进程运行状态的步骤：

步骤1	查看进程运行状态
	# tail -f /var/log/sysappmonitor 2014-10-23 10:00:47 : share_appmonitor_init start 2014-10-23 10:01:36 : l7-feature is down 2014-10-23 10:01:36 : begin to restart l7-feature 1 times 2014-10-23 10:01:42 : /usr/private/l7-feature 1263 2014-10-23 10:01:56 : l7-feature is down 2014-10-23 10:01:56 : begin to restart l7-feature 1 times 2014-10-23 10:02:02 : /usr/private/l7-feature 1495

2.3 查看实时日志信息

对系统出现的 DEBUG 进行实时跟踪，比如 PHP 网页错误，网络故障等

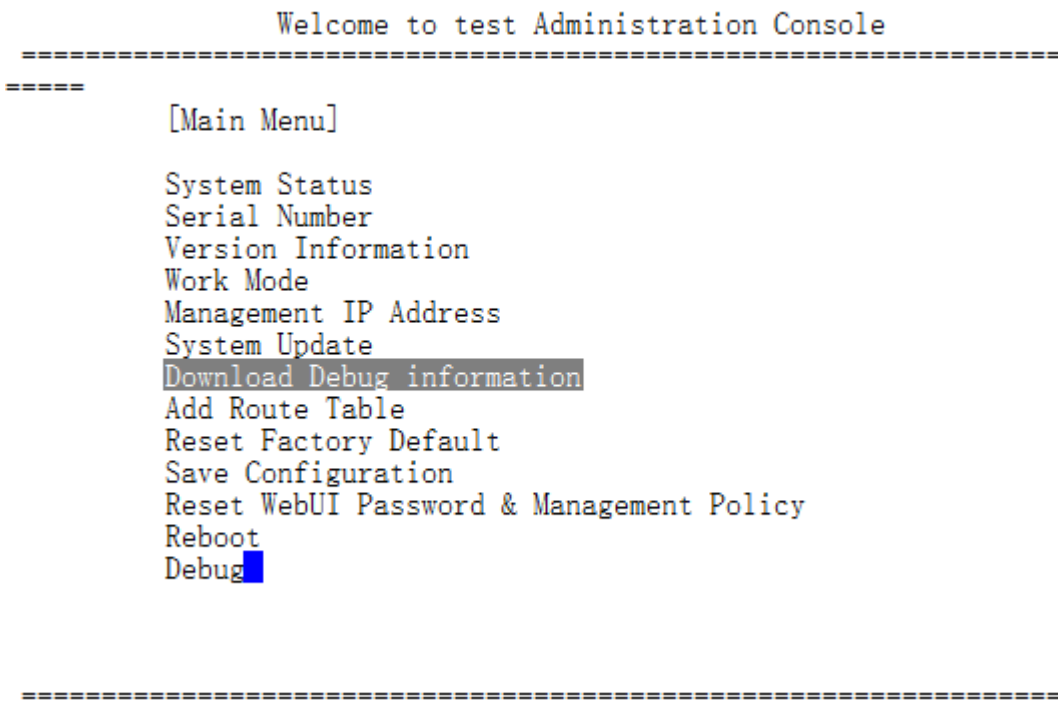
查看日志信息的步骤：

步骤1	查看debug信息
	# tail -f /var/log/messages Oct 23 19:48:20 (none) daemon.err openvpn[11356]: Options error: Unrecognized option or missing parameter(s) in client.conf:43: remote (2.2.2) Oct 23 19:48:20 (none) daemon.warn openvpn[11356]: Use --help for more information. Oct 23 19:48:31 (none) daemon.err openvpn[11413]: Options error: Unrecognized option or missing parameter(s) in client.conf:43: remote (2.2.2) Oct 23 19:48:31 (none) daemon.warn openvpn[11413]: Use --help for

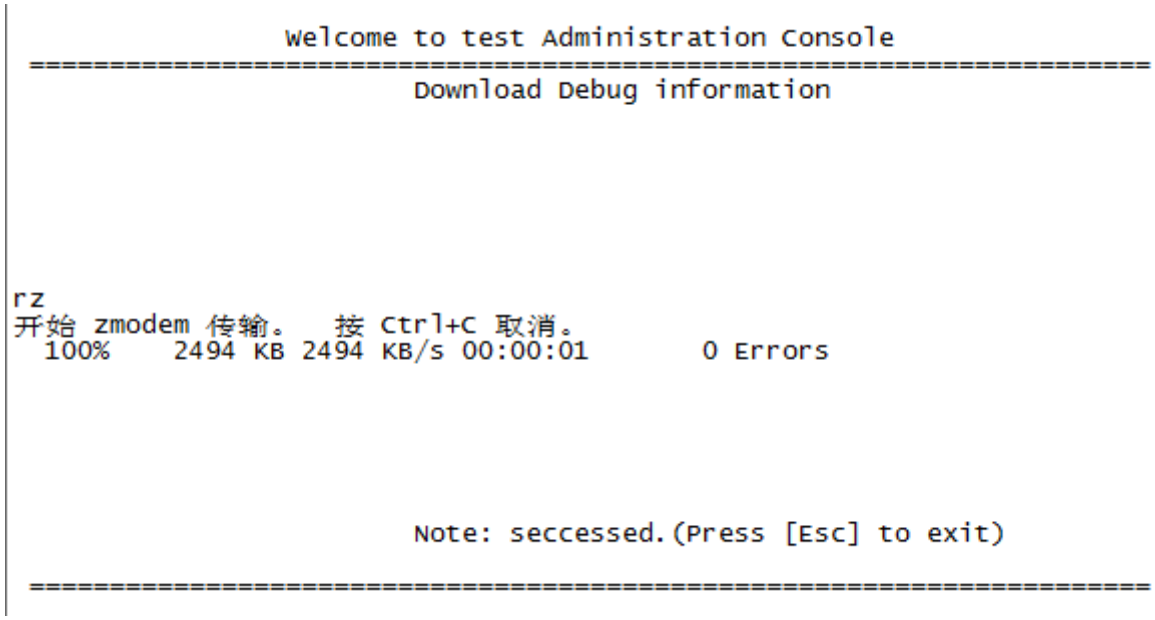
more information.
Oct 23 19:48:40 (none) daemon.err openvpn[11466]: Options error: Unrecognized option or missing parameter(s) in client.conf:43: remote (2.2.2)

2.4 下载实时日志信息

进入后台一级菜单，按上下键选择

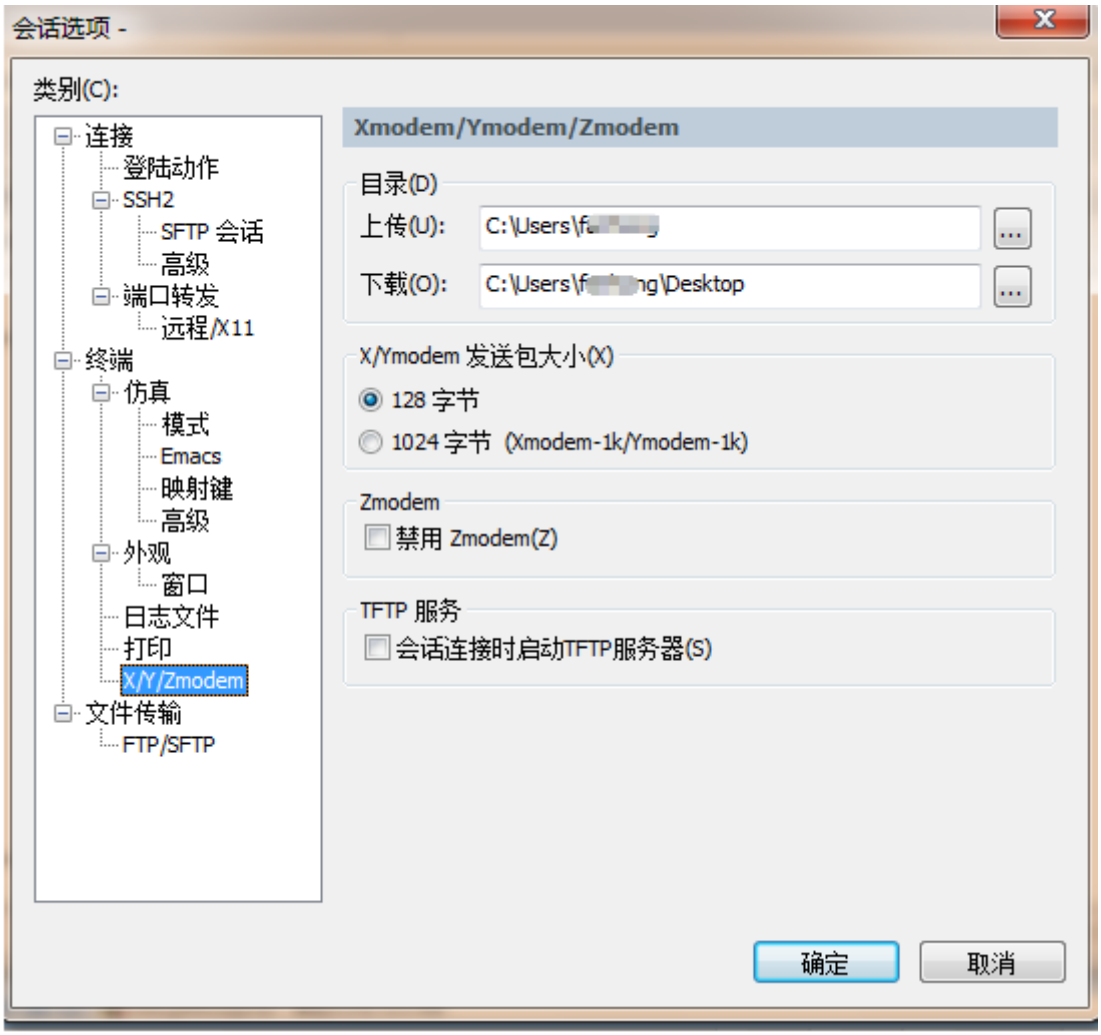


按回车键

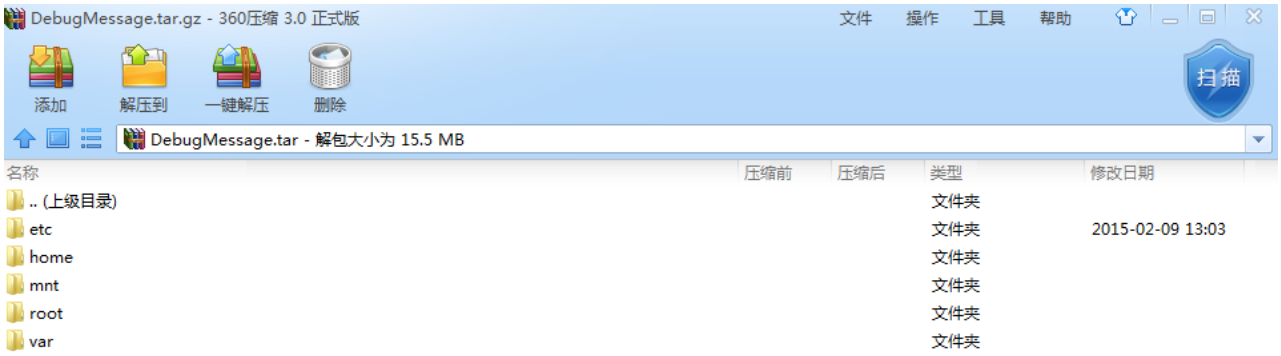


会将设备的调试信息下载至本地目录。

本地目录需在 ssh 工具上设置。



可在本地目录里查看，如下图：


DebugMessage.tar.gz - 360压缩 3.0 正式版
文件
操作
工具
帮助
添加
解压到
一键解压
删除
扫描
DebugMessage.tar - 解包大小为 15.5 MB
名称
压缩前
压缩后
类型
修改日期
.. (上级目录)
文件夹
etc
文件夹
2015-02-09 13:03
home
文件夹
mnt
文件夹
root
文件夹
var
文件夹

3 接口

3.1 配置以太网端口

3.1.1 以太网端口概述

通过配置以太网端口可以实现更改端口的带宽设置、双工模式以及端口速率等设置功能。对于端口的命名，网卡名称前缀为 LAN 或者 WAN，比如 LAN1、WAN1 等等；设备的所有端口缺省状态下是打开的，缺省自协商模式。

3.1.2 配置案例

案例描述

将端口 WAN1 的速率设置为 100Mbps，双工模式设置为全双工，关闭端口 WAN1。

配置步骤：

步骤1	进入以太网端口配置模式
	# ifconfig WAN1
步骤2	重置WAN1网口到自适应模式
	ethtool –r WAN1
步骤3	配置端口WAN1的带宽为100Mbps
	ethtool -s WAN1 speed 100
步骤4	配置端口WAN1为全双工工作模式
	# duplex full
步骤5	关闭端口WAN1
	# ifconfig WAN1 down

3.1.3 故障分析

用如下方法测试以太网端口是否正常工作 :在网络负载小时 ,从 PC 机(PC 机与设备位于同一局域网内 ）Ping 设备的以太网口，观察是否能正确返回全部报文；

在网络负载大时，查看连接双方(如设备和交换机)的端口统计信息，观察接收到错帧的统计数量是否快速增加。

如果这两项测试中有任何一项不能通过，则可以断定设备的以太网口工作不正常。

在确认以太网有故障之后可按如下步骤进行排错：

1) 查看物理设备连接是否正常

2) 在物理设备连接正常的情况下，网线两端端口对应的 Link 指示灯应点亮。

3) 查看连接双方速率设置是否一致

4) 如果一方工作于 100Mbps 模式，而另一方工作于 10Mbps 模式时，端口也不会正常工作。故障表现为：配置为 100Mbps 模式的一方显示为端口 down；配置为 10Mbps 模式的一方则显示为端口 UP。对于这种故障，只要使用 speed 命令把连接双方的速率配成一致即可。

5) 查看连接双方是否处于同一网络

6) 连接双方必须处于同一网络，即二者的网络地址一样而主机地址不同，如果二者网络地址不一样，请用 ip address 命令正确设置 IP 地址。

7) 查看连接双方的双工模式是否一致（其中一方为设备）

当双工模式不一致，即一方工作于全双工模式，而另一方工作于半双工模式，故障表现为：

网络流量增大时，配置为半双工模式的一方显示冲突频繁（如连接共享式 Hub 则整个网络段上所有其它机器都显示冲突严重），配置为全双工模式的一方则显示接收到大量错包，同时，双方丢包严重。

可用 show interface [IFNAME]命令查看以太网收发包的错误率，冲突现象一般可以通过网口状态指示灯观察到；

在连接共享式 Hub 时，应该以半双工模式工作；在连接 Lanswitch 时，一般使用全双工模式工作。

3.2 配置网桥模式

3.2.1 网桥模式概述

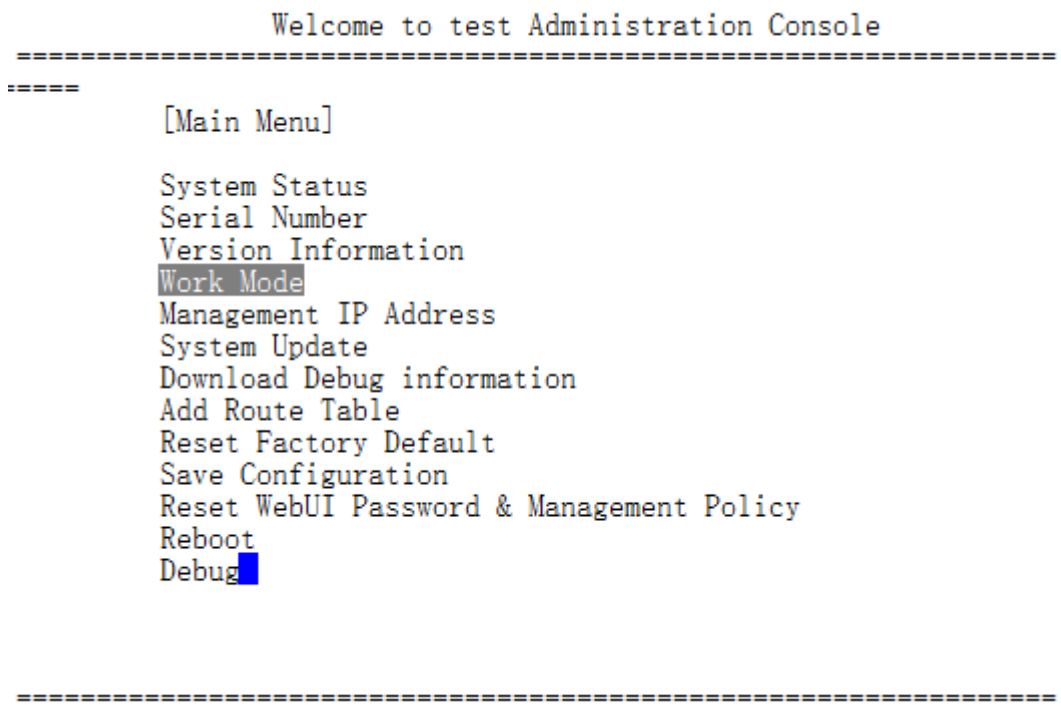
网桥模式功能：最初是由 DEC 公司提出，并被 802.1 委员会采纳并标准化，网桥模式使用最方便，易于安装。当桥接入互连的局域网内，就能运行。它不会影响现存的局域网，原有的软硬件无须改变，也不要设置地址开关和加载路径选择表参数。对于用户来说，该网桥是透明的，即该网桥进入或离开整个网络，用户感觉不到。

网桥模式是把“设备”视为一条带过滤功能的网线使用，把“设备”接在原有网关及内网用户之间，不用更改网络拓扑结构和配置，这种模式于用户可以做到完全“透明”

3.2.2 配置网桥模式

后台页面配置网桥步骤：

1、 登陆到后台配置页面进行网桥模式配置



2、选择 Work Mode 进入工作模式

```
                Welcome to Test-8200 Administration Console
==========================================================================

          [Work Mode]

          0 Route
          1 Bridge
          2 Sniffer

          Current Operation Mode:  1
          Enter Your Choice:  1
          Are you sure(Y-yes,N-no):     y




          Note: The System Will Reboot After Chose Y
==========================================================================
```

根据提示选择序号 1 为 Bridge1 模式，然后重启设备模式，完成配置

4 配置静态路由

4.1 静态路由概述

在 IP 设备中，单播路由的获得通常有两种途径：静态配置和动态路由获取。静态配置就是由网络管理员通过终端命令行等手段明确定义，被称为静态路由。下文仅介绍静态路由相关配置。

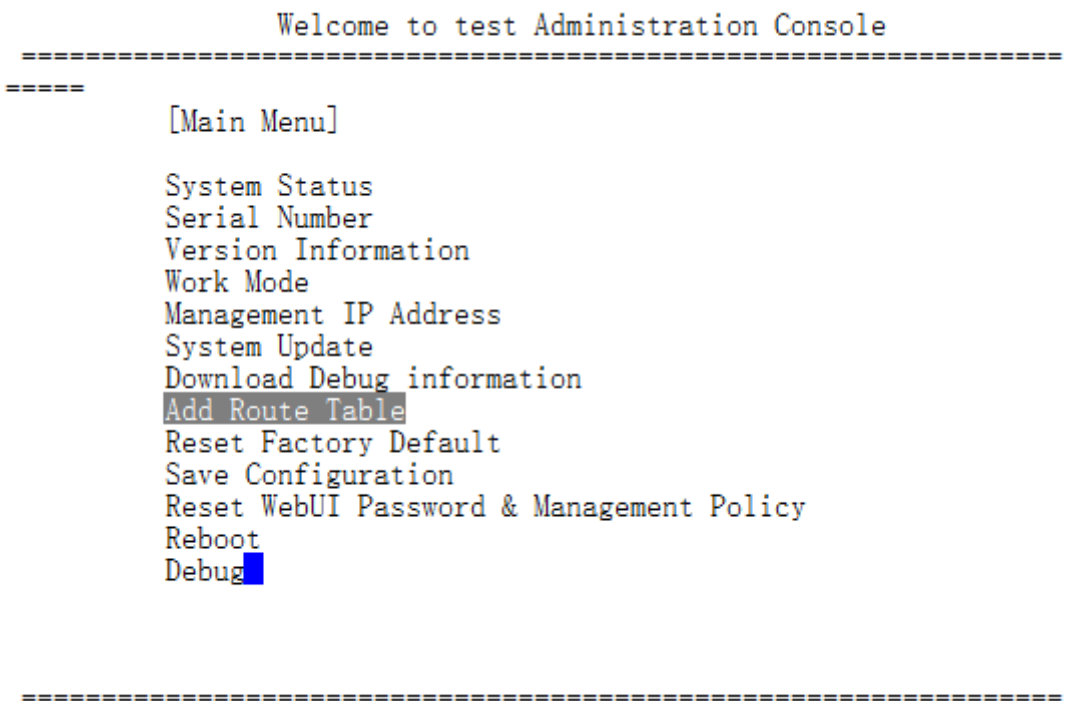
4.1.1 配置静态路由

静态路由是由用户配置的路由。当用户确信到达某个网段应该先转发到某个地址时，可以通过 ip route 命令配置这个静态路由，同时可以配置该静态路由的权重(1-100)，用于负载分担。静态路由支持地址监控对象的联动。当地址监控对象失效以后，使对应的静态路由无效，并增加地址监控对象中的地址的 32 位掩码的路由，下一跳和对应的静态路由的下一跳相同。

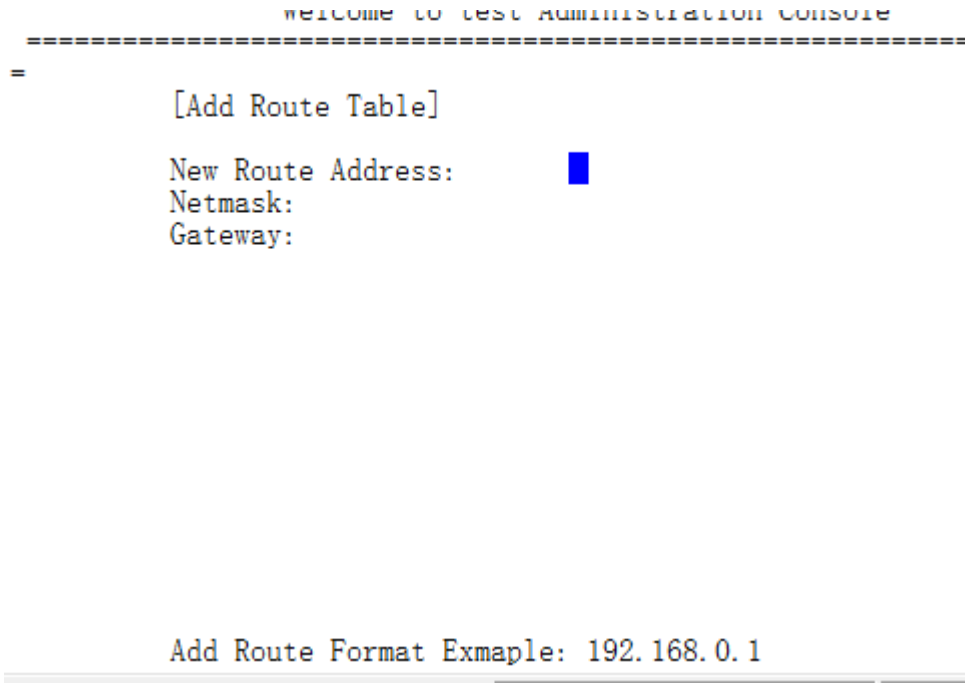
增加路由的方法有两种：

第一种：

登陆系统后台一级菜单，上下键选择菜单 Add Route Table



按回车键



New Route Address：目的地址

Netmask：掩码

Gateway：网关地址

按 Esc 返回上一级菜单。

第二种:

进入命令行，使用 route 命令查询

[HOSTNAME@root]route

[HOSTNAME@root]route–n

如图：

```
[HOSTNAME@root]route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         172.16.161.2    255.255.255.255 UGH   0      0        0 Bridge1
0.0.0.0         172.16.161.2    0.0.0.0         UG    0      0        0 Bridge1
10.8.0.0        0.0.0.0         255.255.255.0   U     0      0        0 tun0
172.16.0.0      0.0.0.0         255.255.0.0     U     0      0        0 Bridge1
192.168.56.0    10.8.0.1        255.255.255.0   UG    0      0        0 tun0
[HOSTNAME@root]
```

例如：要添加默认网关地址为 192.168.12.1 的默认路由，执行以下命令：

route add 0.0.0.0 mask 0.0.0.0 192.168.12.1

添加到目的主机路由：

[HOSTNAME@root]route add 192.168.10.2 gw 192.168.1.1

添加到目标主机路由：

[HOSTNAME@root]route add -net 192.168.10.0 netmask 255.255.255.0 gw 192.168.1.1

添加缺省静态路由：

[HOSTNAME@root]route add default gw 172.16.161.2

删除到目的主机路由：

[HOSTNAME@root]route del 192.168.10.2 gw 192.168.1.1

删除到目标主机路由：

[HOSTNAME@root]route del -net 192.168.10.0 netmask 255.255.255.0 gw 192.168.1.1

删除缺省静态路由：

[HOSTNAME@root]route del default gw 172.16.161.2

5 DNS

5.1 DNS 概述

DNS 为其他需要域名解析的模块提供域名解析客户端功能：向配置的 DNS 服务器发送域名解析请求，并接受 DNS 服务器的响应，最后将解析后的地址发送给各个使用 DNS 的模块。

一般来说不推荐后台配置 DNS，通过后台配置管理 IP，可直接在 web 管理界面**【网络配置】-【DNS 配置】**完成该项配置即可，简单便捷！

5.2 配置 DNS

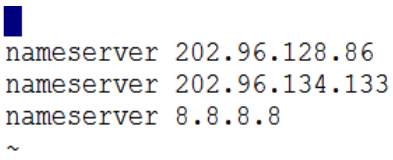
5.2.1 配置主DNS服务器

客户端首先向 DNS 主服务器请求域名解析。

配置方法：

1，进入配置模式进行配置。 vi /etc/resolv.conf

如图：



按下键盘i即可编辑修改你需要的DNS,退出编辑按下ESC，修改成功后输入:wq保存退出即可

2,，直接后台配置方式：echo nameserver A.B.C.D

5.2.2 配置从DNS服务器

如果 DNS 主服务器解析失败或超时，客户端首先向 DNS 从服务器请求域名解析。

配置步骤：

步骤1	vi /etc/resolv.conf	进入配置模式
步骤2	ip name-server backup A.B.C.D	配置从DNS服务器

使用 no ip name-server backup 清除从 DNS 服务器。

5.2.3 DNS查询

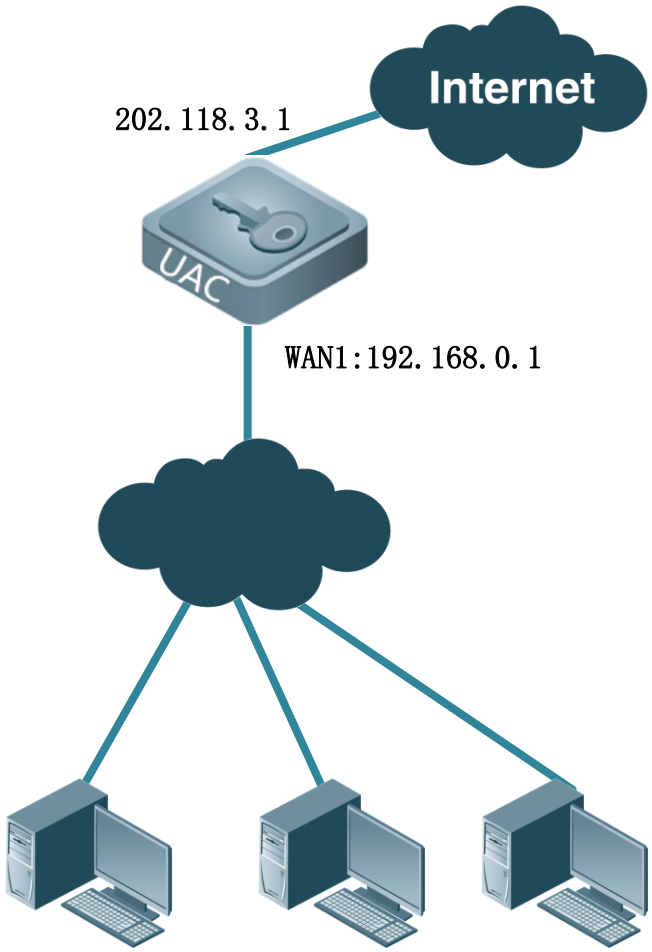
进行域名解析

配置步骤：

步骤1	cat /etc/resolv.conf	进入配置模式
步骤2		域名解析

5.3 配置案例

5.3.1 配置案例:



案例描述

DNS 服务器地址为 202.118.3.2，备份 DNS 服务器地址为 202.118.3.3。在设备上配置 DNS 服务后可以向配置的 DNS 服务器发送域名解析请求，并接受 DNS 服务器的响应，来进行域名解析。

配置步骤：

步骤1	创建一个域。
	# echo "nameeserver 202.118.3.2" >> / etc/resolv.conf # echo "nameeserver 202.118.3.3" >>/ etc/resolv.conf
步骤2	查看配置信息。
	# cat / etc/resolv.conf nameserver 202.118.3.2 nameserver 202.118.3.3

5.4 常见故障分析

5.4.1 故障现象1：DNS解析失败

现象	DNS 解析失败。
分析	DNS服务器配置错误，或没有到DNS服务器的路由。
解决	配置正确的DNS服务器地址或添加到DNS服务器网络的路由。

6 硬盘操作

6.1 Console/SSH 格式化硬盘

UAC 第一次加载系统，会自动检测硬盘是否仅有一个 linux 分区，如果是，脚本不执行格式化操作；如果否，脚本会自行格式化硬盘，完成硬盘初始化。

手动格式化操作是针对硬盘为一个 linux 分区的情况，举例说明，如硬盘容量 500G，分区只有 100G，剩下 400G 没有分区，造成磁盘浪费。

另外一种情况是，UAC 运行了一段时间，正常审计上网行为等日志，突然出现不审计的现象，经检查，后台各项服务正常运行，WEB 管理界面也没有误配置，建议初始化硬盘观察，这项操作**请联系 4008111000 协助处理，并确认是否执行该操作。**

6.1.1 查看硬盘分区、容量

使用 fdisk –l（英文字符 L 的小写）查看硬盘分区及容量

[HOSTNAME@root]**fdisk -l**

Disk /dev/hda: 4034 MB, 4034838528 bytes /系统盘，CF 卡容量

128 heads, 63 sectors/track, 977 cylinders

Units = cylinders of 8064 * 512 = 4128768 bytes

Device Boot	Start	End	Blocks	Id System
/dev/hda1	1	977	3939232+	83 Linux

Disk /dev/sda: 500.1 GB, 500107862016 bytes/硬盘容量 500G

255 heads, 63 sectors/track, 60801 cylinders

Units = cylinders of 16065 * 512 = 8225280 bytes

Device Boot	Start	End	Blocks	Id System	
/dev/sda1	1	60801	488384001	83 Linux	/硬盘一个分区

6.1.2 硬盘卸载

1. 卸载硬盘前，需关闭以下相关的服务：

[HOSTNAME@root]**service appmonitor stop**
Stopping appmonitor...[OK]

[HOSTNAME@root]**service mysql stop**
Shutting down MySQL...[OK]

[HOSTNAME@root]**service Collector stop**
Stopping Collector...[OK]

[HOSTNAME@root]**service Scheduler stop**
Stopping Scheduler...[OK]

2. 卸载硬盘
[HOSTNAME@root]**umount /mnt** （卸载硬盘）
[HOSTNAME@root]df （查看硬盘是否挂载）

Filesystem	1K-blocks	Used	Available	Use%	Mounted on
/dev/root	2014032	1017128	894596	53%	/
tmpfs	1682084	0	1682084	0%	/dev/shm
tmpfs	1682084	4	1682080	0%	/tmp

如果硬盘卸载不掉如：
[X@root]**umount /mnt**
umount: can't umount /mnt: Device or resource busy

使用 **fuser -m /mnt** 查看哪些相关进程还活着
kill -9 进程 ID 强制杀掉进程
例如：
[X@root]**fuser -m /mnt**
16284 1503 897 895 734 340 303 122 /进程 ID 仅供参考，以实际进程 ID 为准
[X@root]kill -9 16284 1503 897 895 734 340 303 122
[X@root]**umount /mnt**

6.1.3 硬盘分区

默认情况下系统会自动初始化（分区+格式化）硬盘，一般是在硬盘不能挂载，存储审计数据的情况下，

才会选择手动分区/格式化硬盘。

硬盘分区

[HOSTNAME@root]**fdisk /dev/sda1**

The number of cylinders for this disk is set to 19457.

There is nothing wrong with that, but this is larger than 1024,

and could in certain setups cause problems with:

1) software that runs at boot time (e.g., old versions of LILO)

2) booting and partitioning software from other OSs

(e.g., DOS FDISK, OS/2 FDISK)

Command (m for help): m/m 为命令帮助提示，一下主要介绍常用命令

Command Action

a toggle a bootable flag

b edit bsd disklabel

c toggle the dos compatibility flag

d delete a partition /删除分区用

l list known partition types

n add a new partition /新建分区

o create a new empty DOS partition table /创建 DOS 分区表

p print the partition table

q quit without saving changes

s create a new empty Sun disklabel

t change a partition's system id

u change display/entry units

v verify the partition table

w write table to disk and exit/写分区表到磁盘

x extra functionality (experts only)

Command (m for help): o

Building a new DOS disklabel. Changes will remain in memory only,

until you decide to write them. After that the previous content

won't be recoverable.

The number of cylinders for this disk is set to 19457.

There is nothing wrong with that, but this is larger than 1024,

and could in certain setups cause problems with:

1) software that runs at boot time (e.g., old versions of LILO)

2) booting and partitioning software from other OSs

(e.g., DOS FDISK, OS/2 FDISK)

Command (m for help): n

Command action

e extended

p primary partition (1-4)

p/输入 p，即选择主分区

Partition number (1-4): 1

First cylinder (1-19457, default 1): Using default value 1（这一步默认，回车就好）

Last cylinder or +size or +sizeM or +sizeK (1-19457, default 19457): Using default value 19457（这一步默认，回车就好）

Command (m for help): w

The partition table has been altered!

Calling ioctl() to re-read partition table

SCSI device sda: 312581808 512-byte hdwr sectors (160042 MB)

sda: Write Protect is off

SCSI device sda: drive cache: write back

现在可以格式化硬盘了，

6.1.4 硬盘格式化

以上操作完成，可执行硬盘格式化

[HOSTNAME@root]**mke2fs -j -b 4096 -i 4096 /dev/sda1**

等格式化完成，回到[HOSTNAME@root]命令行

再[HOSTNAME@root]**reboot**/重启设备

设备起来后检查 reporter 访问是否正常。

6.1.5 查看硬盘是否挂载

设备 license 过期之后，设备启动，命令行仍然可以进入

登陆用户名：admin　密码：firewall**（注：如果 web 页面的 admin 用户密码修改，则会跟着修改该后台密码）**=====

```
                Welcome to test Administration Console
 ================================================================================
=====
          [Main Menu]

          System Status
          Serial Number
          Version Information
          Work Mode
          Management IP Address
          System Update
          Download Debug information
          Add Route Table
          Reset Factory Default
          Save Configuration
          Reset WebUI Password & Management Policy
          Reboot
          Debug


 ================================================================================
```

用户名：admin　密码：Login*PWD

方法一 进入之后输入命令 fdisk –l(英文小写字母)，然后 df 查看硬盘是否挂载，

这是硬盘有接好

```
[HOSTNAME2@superman]
[HOSTNAME2@superman]fdisk -l

Disk /dev/hda: 2065 MB, 2065932288 bytes
64 heads, 62 sectors/track, 1016 cylinders
Units = cylinders of 3968 * 512 = 2031616 bytes

   Device Boot      Start         End      Blocks  Id System
/dev/hda1               1        1016     2015713  83 Linux

Disk /dev/sda: 320.0 GB, 320072933376 bytes
255 heads, 63 sectors/track, 38913 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot      Start         End      Blocks  Id System
/dev/sda1               1       38913   312568641  83 Linux
[HOSTNAME2@superman]
```

1，如下情况正常硬盘被识别

使用 df 命令查看硬盘挂载情况：

```
          4000                0                   0
[HOSTNAME2@superman]
[HOSTNAME2@superman]df
Filesystem           1K-blocks      Used Available Use% Mounted on
/dev/root              1983984   1079896    803304  57% /
tmpfs                  1020036         0   1020036   0% /dev/shm
tmpfs                  1020036     28600    991436   3% /tmp
/dev/sda1            302779320    631104 286519784   0% /mnt
[HOSTNAME2@superman]
```

2，

如下情况不正常，硬盘有接好并识别到，没有挂载

```
[HOSTNAME2@superman]
[HOSTNAME2@superman]fdisk -l

Disk /dev/hda: 2065 MB, 2065932288 bytes
64 heads, 62 sectors/track, 1016 cylinders
Units = cylinders of 3968 * 512 = 2031616 bytes

   Device Boot      Start         End      Blocks  Id System
/dev/hda1               1        1016     2015713  83 Linux

Disk /dev/sda: 320.0 GB, 320072933376 bytes
255 heads, 63 sectors/track, 38913 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot      Start         End      Blocks  Id System
/dev/sda1               1       38913   312568641  83 Linux
[HOSTNAME2@superman]
```

```
[HOSTNAME2@superman]
[HOSTNAME2@superman]df
Filesystem           1K-blocks      Used Available Use% Mounted on
/dev/root              1983984   1079992    803208  57% /
tmpfs                  1020036         0   1020036   0% /dev/shm
tmpfs                  1020036     28596    991440   3% /tmp
[HOSTNAME2@superman]
```

方法二 判断硬盘有没有被识别,

1，如下情况不正常只有 cf 卡没有硬盘

```
[HOSTNAME2@superman]
[HOSTNAME2@superman]
[HOSTNAME2@superman]
[HOSTNAME2@superman]fdisk -l

Disk /dev/hda: 2065 MB, 2065932288 bytes
64 heads, 62 sectors/track, 1016 cylinders
Units = cylinders of 3968 * 512 = 2031616 bytes

   Device Boot      Start         End      Blocks  Id System
/dev/hda1               1        1016     2015713  83 Linux
[HOSTNAME2@superman]
```

2，，如下的情况属于正常，cf 卡和硬盘都被识别

```
[HOSTNAME2@superman]
[HOSTNAME2@superman]fdisk -l

Disk /dev/hda: 2065 MB, 2065932288 bytes
64 heads, 62 sectors/track, 1016 cylinders
Units = cylinders of 3968 * 512 = 2031616 bytes

   Device Boot      Start         End      Blocks  Id System
/dev/hda1               1        1016     2015713  83 Linux

Disk /dev/sda: 320.0 GB, 320072933376 bytes
255 heads, 63 sectors/track, 38913 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot      Start         End      Blocks  Id System
/dev/sda1               1       38913   312568641  83 Linux
[HOSTNAME2@superman]
```

7 系统维护

系统维护包括管理设定、时间设定、系统升级、系统重启及系统相关配置的备份恢复。

7.1 系统时间设定

7.1.1 查看系统连续运行的时间

查看步骤：

步骤1	查看系统连续运行的时间
## uptime 04:03:58 up 10 days, 13:19, 1 user, load average: 0.54, 0.40, 0.20 表示当前时间是上午04:03:58，系统运行已经10天13小时19分钟	

7.1.2 查看系统当前的日期和时间

查看步骤：

步骤1	查看系统当前的日期和时间
#	date Thu Oct 23 20:00:11 CST 2014

7.1.3 查看系统当前的时区

查看步骤：

步骤1　查看系统当前的时区

date -R

Thu, 23 Oct 2014 20:02:31 +0800

表示当前时区为第57时区(即CST,中国时区)。

时区参数对应如下：

1　zone1=GMT-12:00 日界线西

2　zone2=GMT-11:00 中途岛　萨摩亚群岛

3　zone3=GMT-10:00 夏威夷

4　zone4=GMT-09:00 阿拉斯加

5　zone5=GMT-08:00 太平洋时间(美国和加拿大) 蒂华纳

6　zone6=GMT-07:00 山地时间(美国和加拿大)

7　zone7=GMT-07:00 亚利桑那

8　zone8=GMT-07:00 齐瓦瓦 拉巴斯 马扎特兰

9　zone9=GMT-06:00 萨斯喀彻温

10　zone10=GMT-06:00 中部时间(美国和加拿大)

11　zone11=GMT-06:00 中美州

12　zone12=GMT-06:00 瓜达拉哈拉 墨西哥城 蒙特雷

13　zone13=GMT-05:00 波哥大　利马 基多

14　zone14=GMT-05:00 东部时间(美国和加拿大)

15　zone15=GMT-05:00 印第安那州(东部)

16　zone16=GMT-04:00 大西洋时间(美国和加拿大)

17　zone17=GMT-04:00 加拉加斯　拉巴斯

18　zone18=GMT-04:00 圣地亚哥

19 zone19=GMT-03:30 纽芬兰

20 zone20=GMT-03:00 巴西利亚

21 zone21=GMT-03:00 布宜诺斯艾利斯 乔治敦

22 zone22=GMT-03:00 格陵兰

23 zone23=GMT-02:00 中大西洋

24 zone24=GMT-01:00 佛得角群岛

25 zone25=GMT-01:00 亚速尔群岛

26 zone26=GMT 格林威治 都柏林 爱丁堡 伦敦 里斯本

27 zone27=GMT 卡萨布兰卡 蒙罗维亚

28 zone28=GMT+01:00 阿姆斯特丹 柏林 伯尔尼 罗马 斯德哥尔摩 维也纳

29 zone29=GMT+01:00 贝尔格莱德 布拉迪斯拉发 布达佩斯 卢布尔雅那

30 zone30=GMT+01:00 布鲁塞尔 哥本哈根 马德里 巴黎

31 zone31=GMT+01:00 萨拉热窝 斯科普里 华沙 萨格勒布

32 zone32=GMT+01:00 中非西部

33 zone33=GMT+02:00 布加勒斯特

34 zone34=GMT+02:00 哈拉雷 比勒陀利亚

35 zone35=GMT+02:00 赫尔辛基 基辅 里加 索非亚 塔林 维尔纽斯

36 zone36=GMT+02:00 开罗

37 zone37=GMT+02:00 雅典 贝鲁特 伊斯坦布尔 明斯克

38 zone38=GMT+02:00 耶路撒冷

39 zone39=GMT+03:00 巴格达

40 zone40=GMT+03:00 科威特 利雅得

41 zone41=GMT+03:00 莫斯科 圣彼得堡 伏尔加格勒

42 zone42=GMT+03:00 内罗毕

43 zone43=GMT+03:30 德黑兰

44 zone44=GMT+04:00 阿布扎比 马斯喀特

45 zone45=GMT+04:00 巴库 第比利斯 埃里温

46 zone46=GMT+04:30 喀布尔

47 zone47=GMT+05:00 叶卡捷琳堡

48 zone48=GMT+05:00 伊斯兰堡 卡拉奇 塔什干

49 zone49=GMT+05:30 马德拉斯 孟买 加尔各答 新德里

50 zone50=GMT+05:45 加德满都

51 zone51=GMT+06:00 阿拉木图 新西伯利亚

52 zone52=GMT+06:00 阿斯塔纳 达卡

53 zone53=GMT+06:00 斯里哈亚华登尼普拉

54 zone54=GMT+06:30 仰光

55 zone55=GMT+07:00 克拉斯诺亚尔斯克

56 zone56=GMT+07:00 曼谷 河内 雅加达

57 zone57=GMT+08:00 北京 重庆 乌鲁木齐 香港特别行政区

58 zone58=GMT+08:00 吉隆坡 新加坡

59 zone59=GMT+08:00 珀斯

60 zone60=GMT+08:00 台北

61 zone61=GMT+08:00 伊尔库茨克 乌兰巴图

62 zone62=GMT+09:00 大阪 东京 札幌

63 zone63=GMT+09:00 汉城

64 zone64=GMT+09:00 雅库次克

65 zone65=GMT+09:30 阿德莱德

66 zone66=GMT+09:30 达尔文

67 zone67=GMT+10:00 布里斯班

68 zone68=GMT+10:00 符拉迪沃斯托克

69 zone69=GMT+10:00 关岛 莫尔兹比港

70 zone70=GMT+10:00 霍巴特

71 zone71=GMT+10:00 堪培拉 墨尔本 悉尼

72 zone72=GMT+11:00 马加丹 所罗门群岛 新喀里多尼亚

73 zone73=GMT+12:00 奥克兰 惠灵顿

74 zone74=GMT+12:00 斐济 堪察加半岛 马绍尔群岛

75 zone75=GMT+13:00 努库阿洛法

7.1.4 手动设置系统当前的日期和时间

命令说明：

hwclock - set - date= "10/23/2014 20:12"

Thu Oct 23 20:12:59 2014 0.000000 seconds

关键字和参数	说明
<2014>	配置年份
<10>	配置月份
<23>	配置日
<20>	配置小时
<12>	配置分钟

配置步骤：

步骤1	
	设置系统当前的日期和时间
	# date 2010 04 02 10 20 50
	表示设置系统时间为2010年4月2日上午10点20分50秒

7.2 故障排除

7.2.1 tcpdump抓包命令格式

tcpdump 采用命令行方式，它的命令格式为：[1]

tcpdump [-adeflnNOpqStvx] [-c 数量] [-F 文件名]

[-i 网络接口] [-r 文件名] [-s snaplen]

[-T 类型] [-w 文件名] [表达式]

1. tcpdump 的选项介绍

-a、将网络地址和广播地址转变成名字；

-d、将匹配信息包的代码以人们能够理解的汇编格式给出；

-dd、将匹配信息包的代码以 C 语言程序段的格式给出；

-ddd、将匹配信息包的代码以十进制的形式给出；

-e、在输出行打印出数据链路层的头部信息；

-f、将外部的 Internet 地址以数字的形式打印出来；

-l、使标准输出变为缓冲行形式；

-n、不把网络地址转换成名字；

-t、在输出的每一行不打印时间戳；

-v 、输出一个稍微详细的信息，例如在 ip 包中可以包括 ttl 和服务类型的信息；

-vv、 输出详细的报文信息；

-c 、在收到指定的包的数目后，tcpdump 就会停止；

-F、 从指定的文件中读取表达式,忽略其它的表达式；

-i、 指定监听的网络接口；

-r、 从指定的文件中读取包(这些包一般通过-w 选项产生)；

-w、 直接将包写入文件中，并不分析和打印出来；

-T、将监听到的包直接解释为指定的类型的报文，常见的类型有 rpc （远程过程调用）和 snmp（简单 网络管理协议；）

下面的例子全是以抓取 LAN1 接口为例

1、 抓取包含 172.16.1.122 的数据包

tcpdump-iLAN1-vnnhost172.16.1.122

2、 抓取包含 172.16.1.0/24 网段的数据包

tcpdump-iLAN1-vnnnet172.16.1.0/24

3、 抓取包含端口 22 的数据包

tcpdump-iLAN1-vnnport22

4、 抓取 udp 协议的数据包

tcpdump-iLAN1-vnnudp

5、 抓取 icmp 协议的数据包

tcpdump-iLAN1-vnnicmp

6、 抓取 arp 协议的数据包

tcpdump-iLAN1-vnnarp

7、 抓取 ip 协议的数据

tcpdump-iLAN1-vnnip

8、 抓取源 ip 是 172.16.1.122 数据包

tcpdump-iLAN1-vnnsrchost172.16.1.122

9、 抓取目的 ip 是 172.16.1.122 数据包

tcpdump-iLAN1-vnndsthost172.16.1.122

10、 抓取源端口是 22 的数据包

tcpdump-iLAN1-vnnsrcport22

11、抓取源 ip 是 172.16.1.253 且目的 ip 是 22 的数据包

tcpdump-iLAN1-vnnsrchost172.16.1.253anddstport22

12、抓取源 ip 是 172.16.1.122 或者包含端口是 22 的数据包

tcpdump-iLAN1-vnnsrchost172.16.1.122orport22

13、抓取源 ip 是 172.16.1.122 且端口不是 22 的数据包

tcpdump-iLAN1-vnnsrchost172.16.1.122andnotport22

14、抓取源 ip 是 172.16.1.2 且目的端口是 22，或源 ip 是 172.16.1.65 且目的端口是 80 的数据包

tcpdump-iLAN1-vnn\(srchost172.16.1.2anddstport22\)or\(srchost172.16.1.65anddstport80\)

15、抓取源 ip 是 172.16.1.59 且目的端口是 22，或源 ip 是 172.16.1.68 且目的端口是 80 的数据包

tcpdump-iLAN1-vnnsrchost172.16.1.59anddstport22orsrchost172.16.1.68anddstport80

16、把抓取的数据包记录存到/tmp/fill 文件中，当抓取 100 个数据包后就退出程序

tcpdump–iLAN1-vnn-w/tmp/fil1-c100

17、从/tmp/fill 记录中读取 tcp 协议的数据包

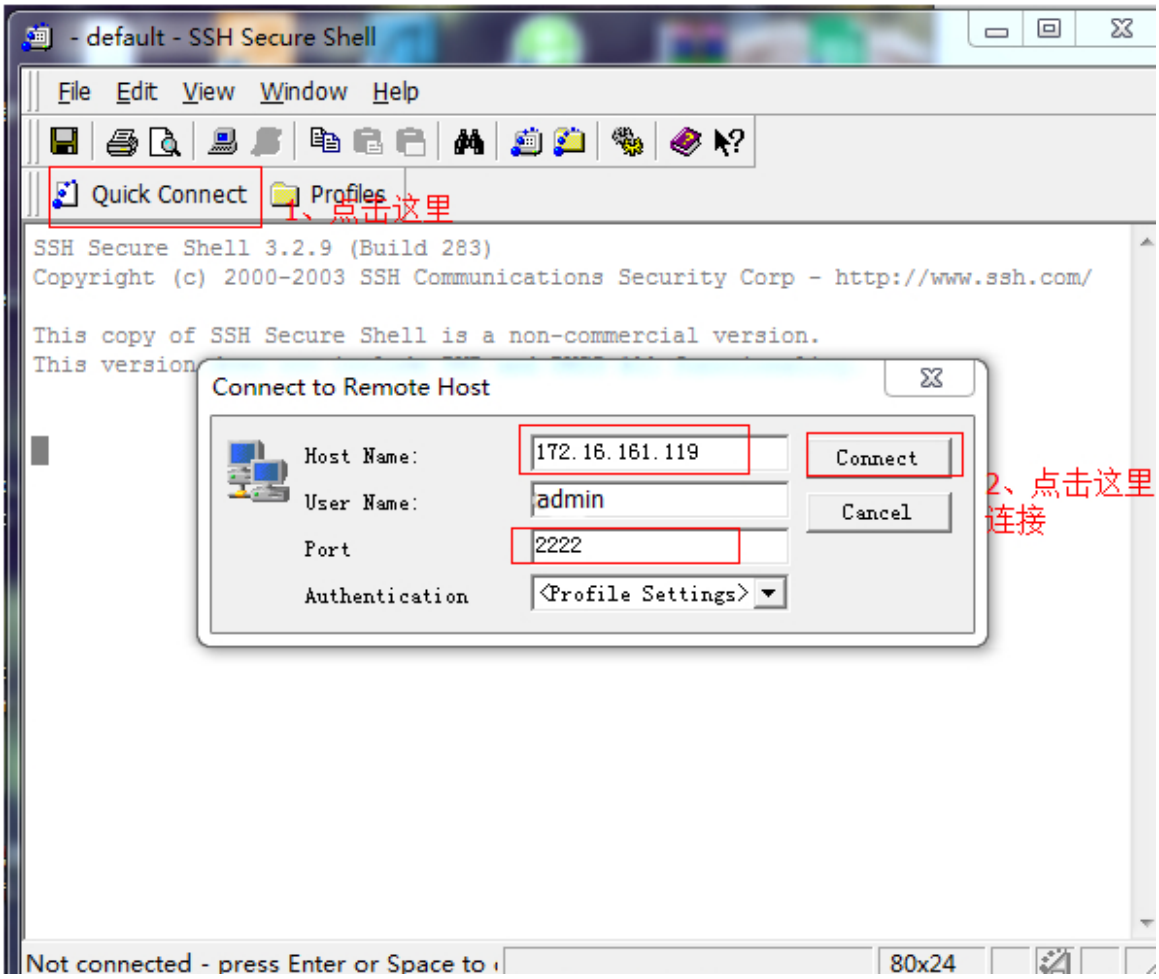
tcpdump–iLAN1-vnn-r/tmp/fil1tcp

18、从/tmp/fill 记录中读取包含 172.16.1.58 的数据包

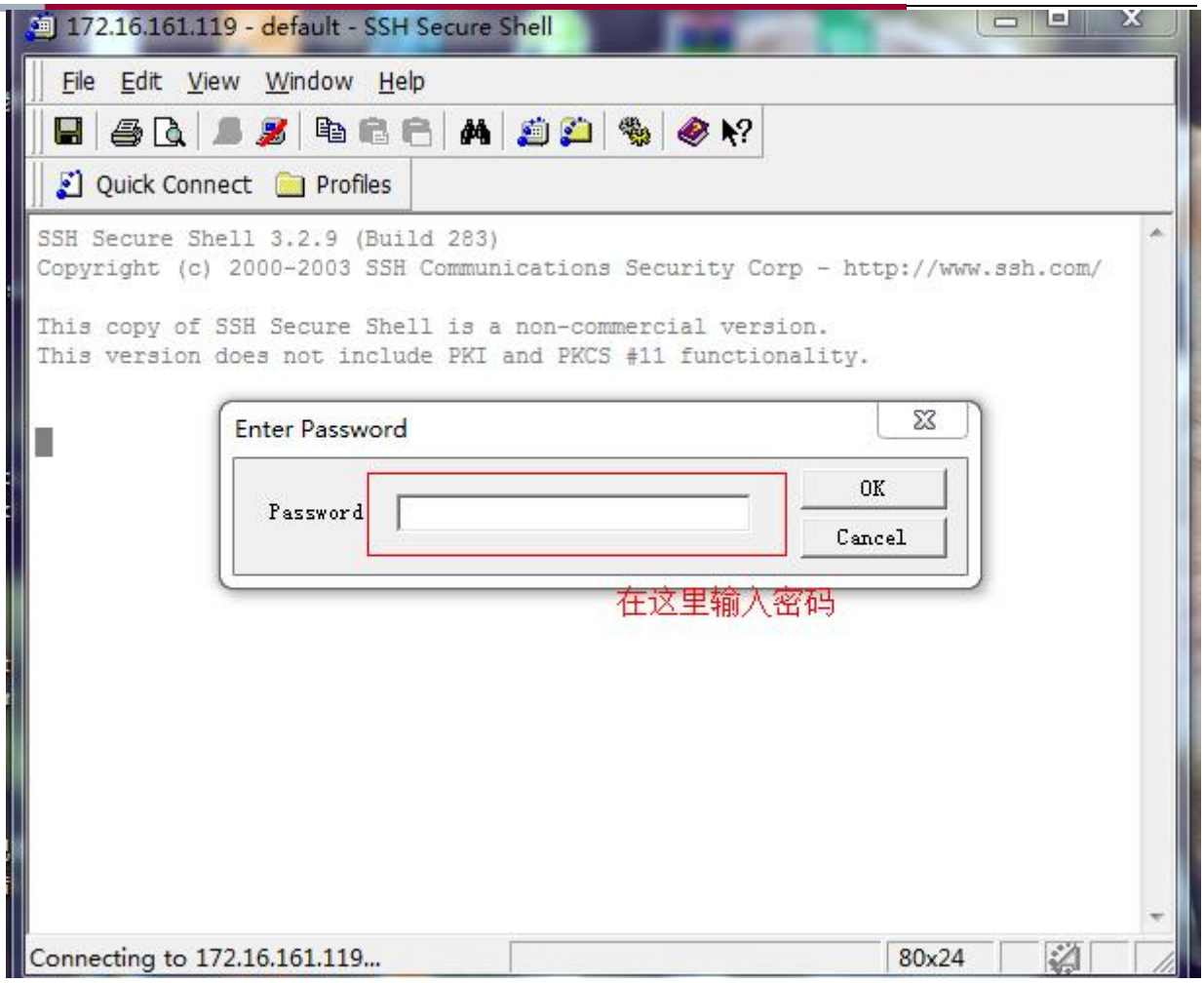
tcpdump–iLAN1-vnn-r/tmp/fil1host172.16.1.58

7.2.2 捕获数据包

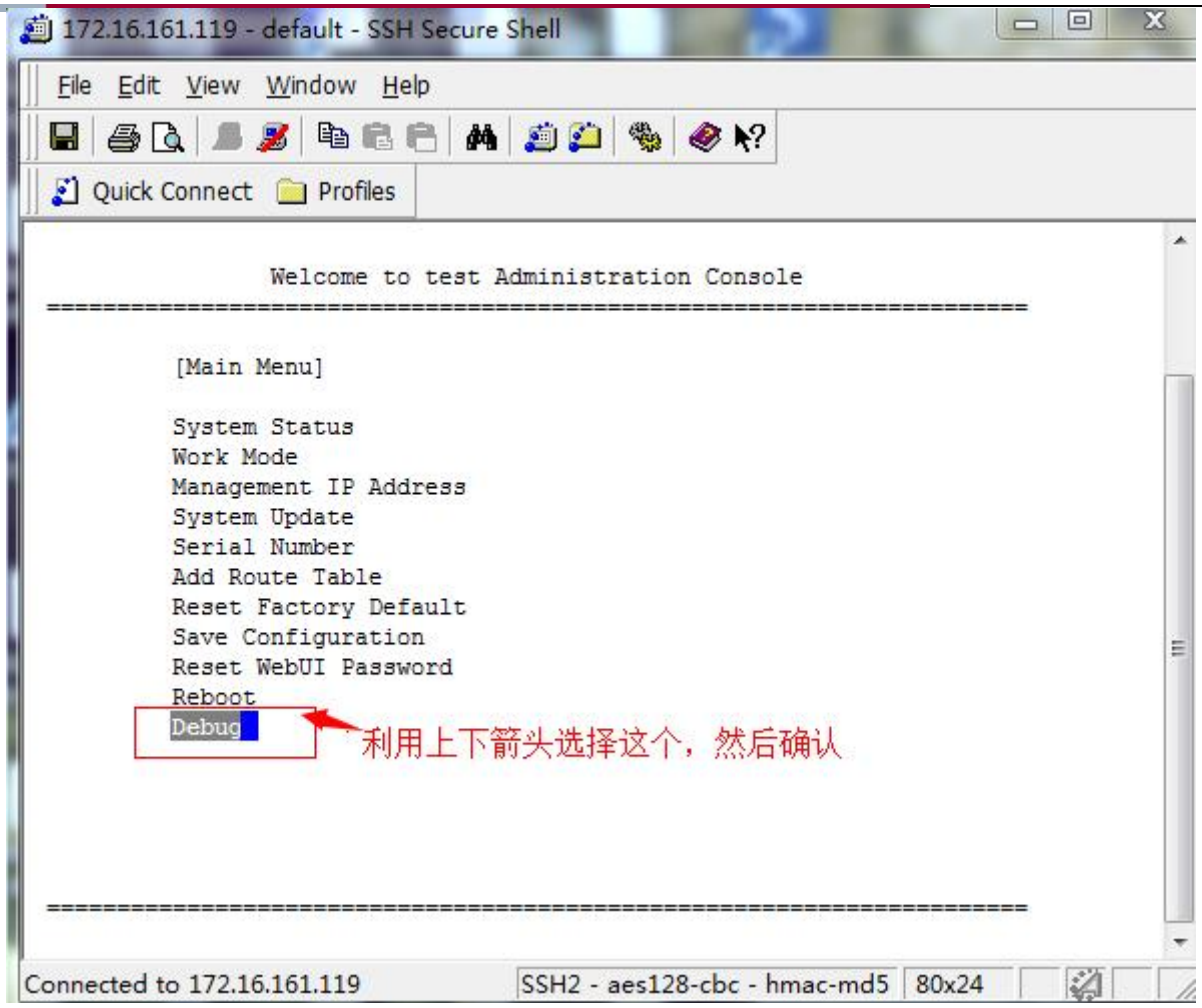
1、点击这个软件打开，然后选择连接



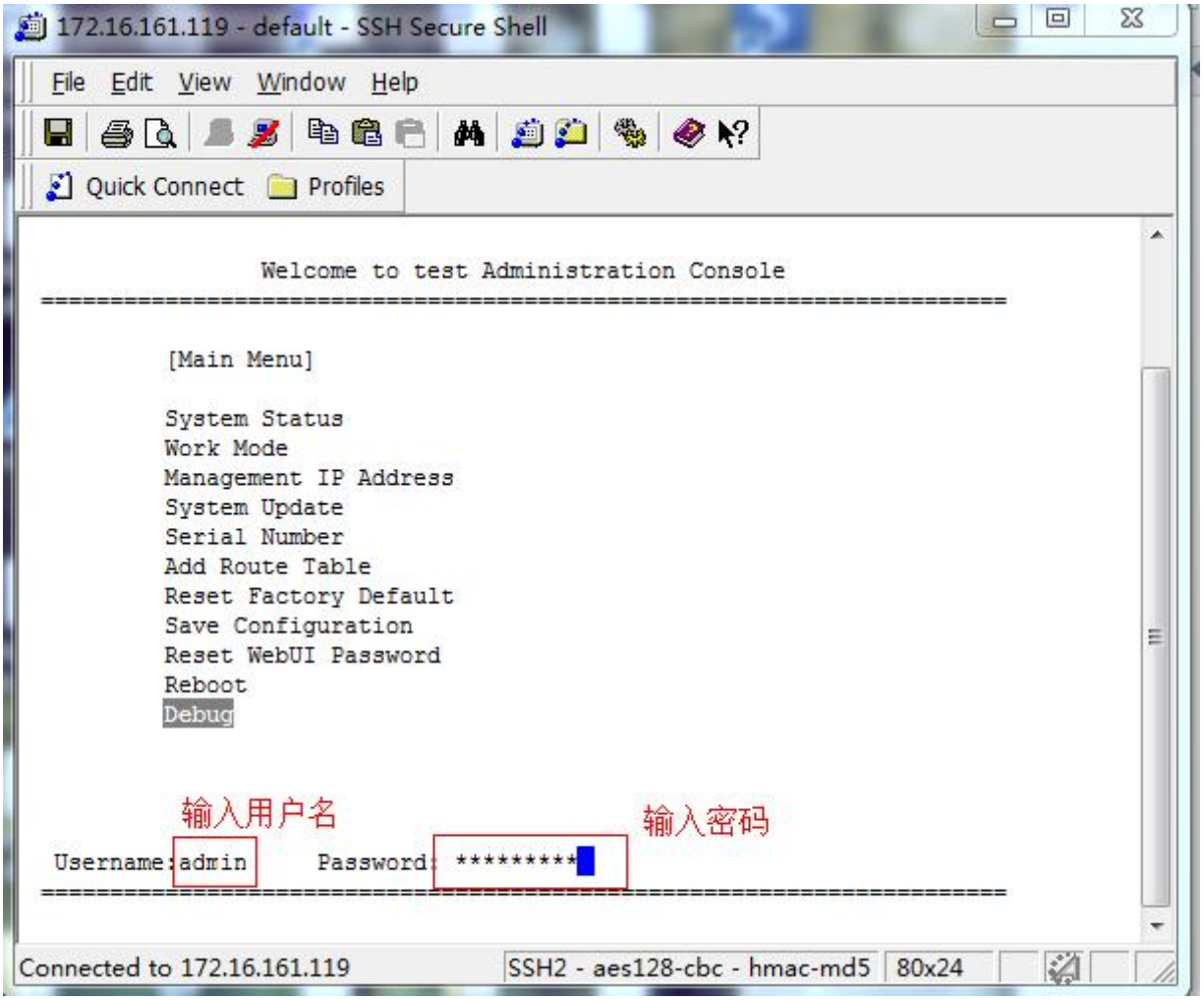
随后会弹出一个窗口需要你输入密码，



密码是：firewall**（注：如果 web 页面的 admin 用户密码修改，则会跟着修改该后台密码）**，密码输入完成后点击 OK。然后进入这个界面，

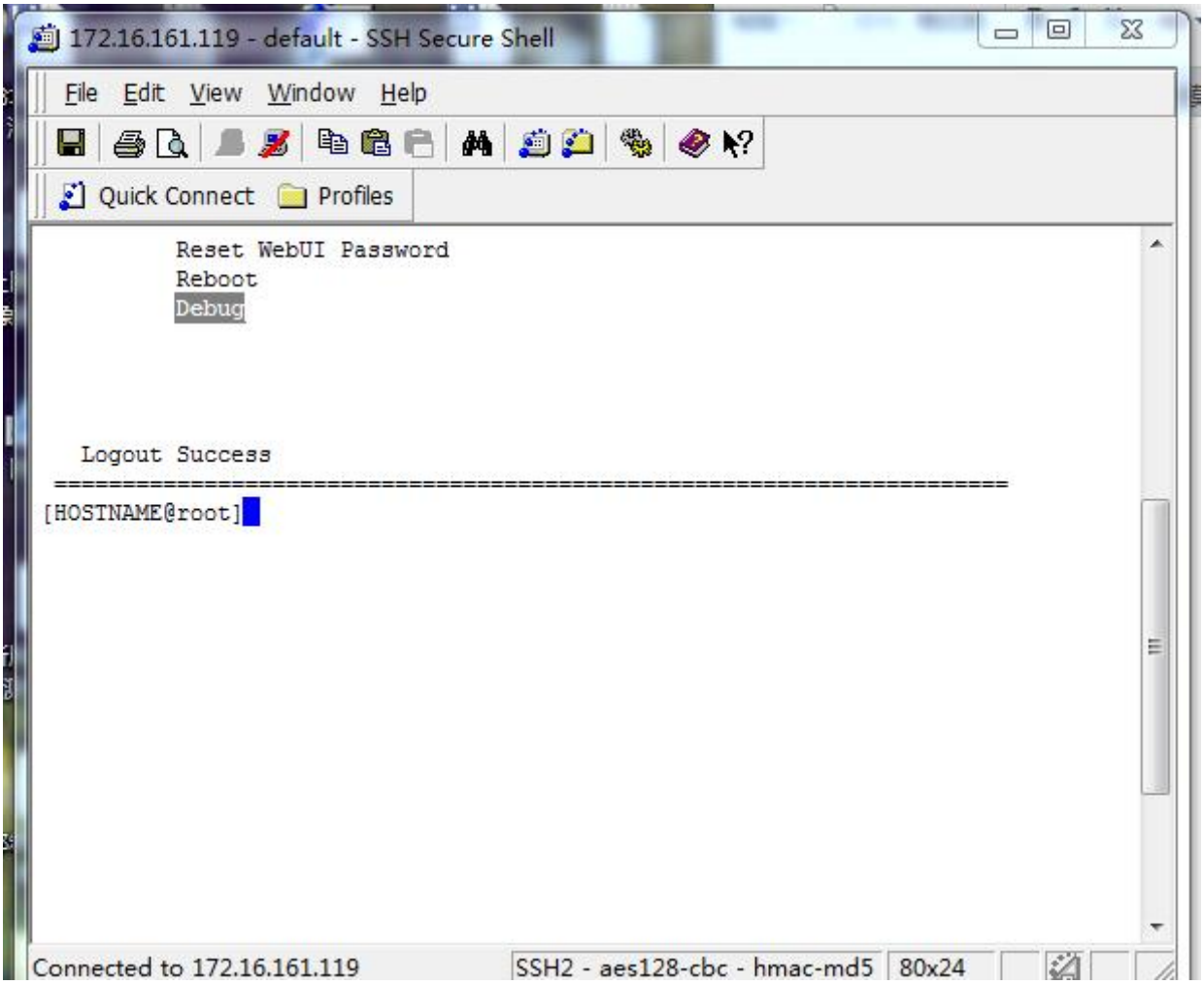


确认后，会要输入用户名和密码，



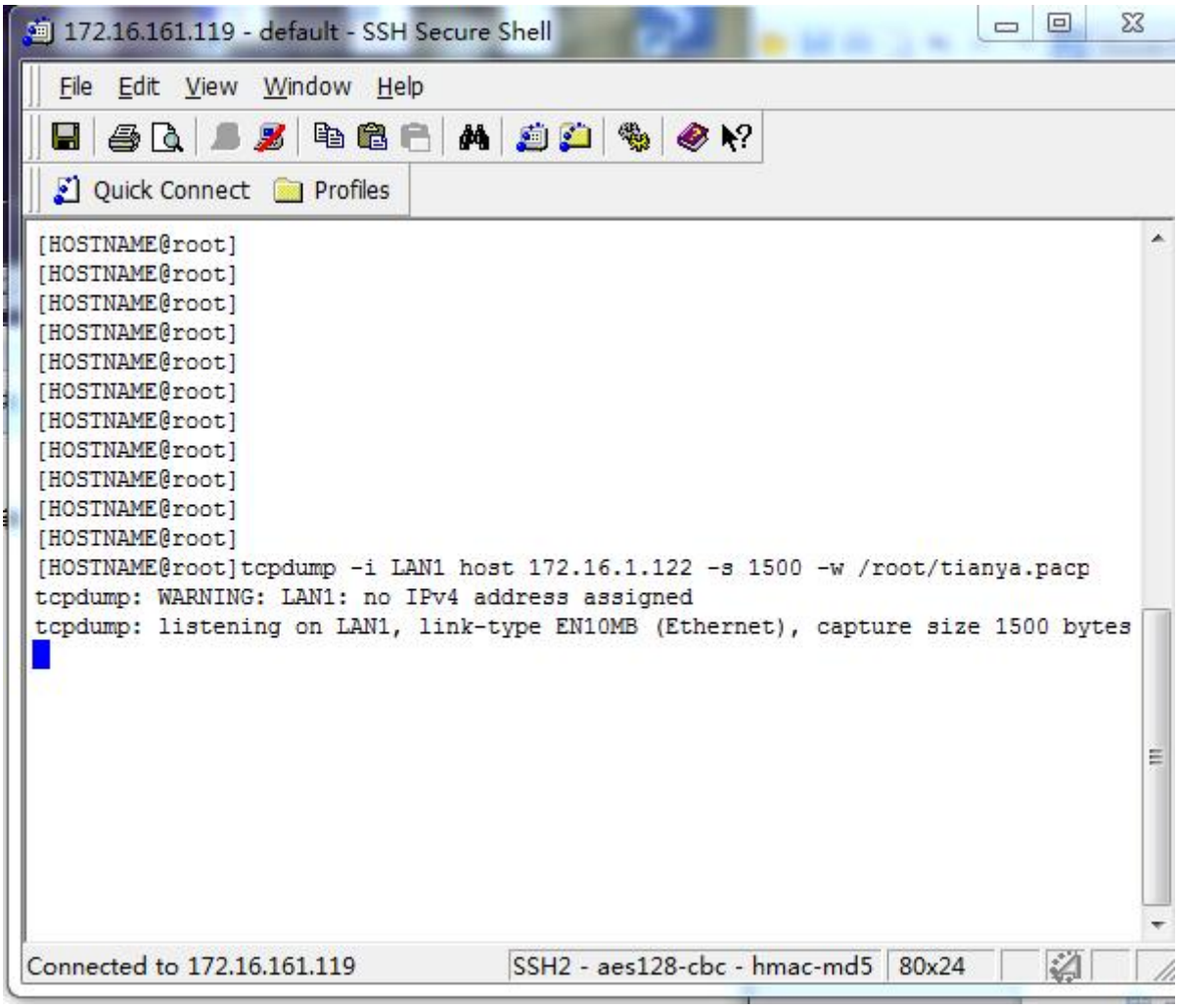
用户名是：admin 密码是：Login*PWD

随后登录成功，进入这个界面



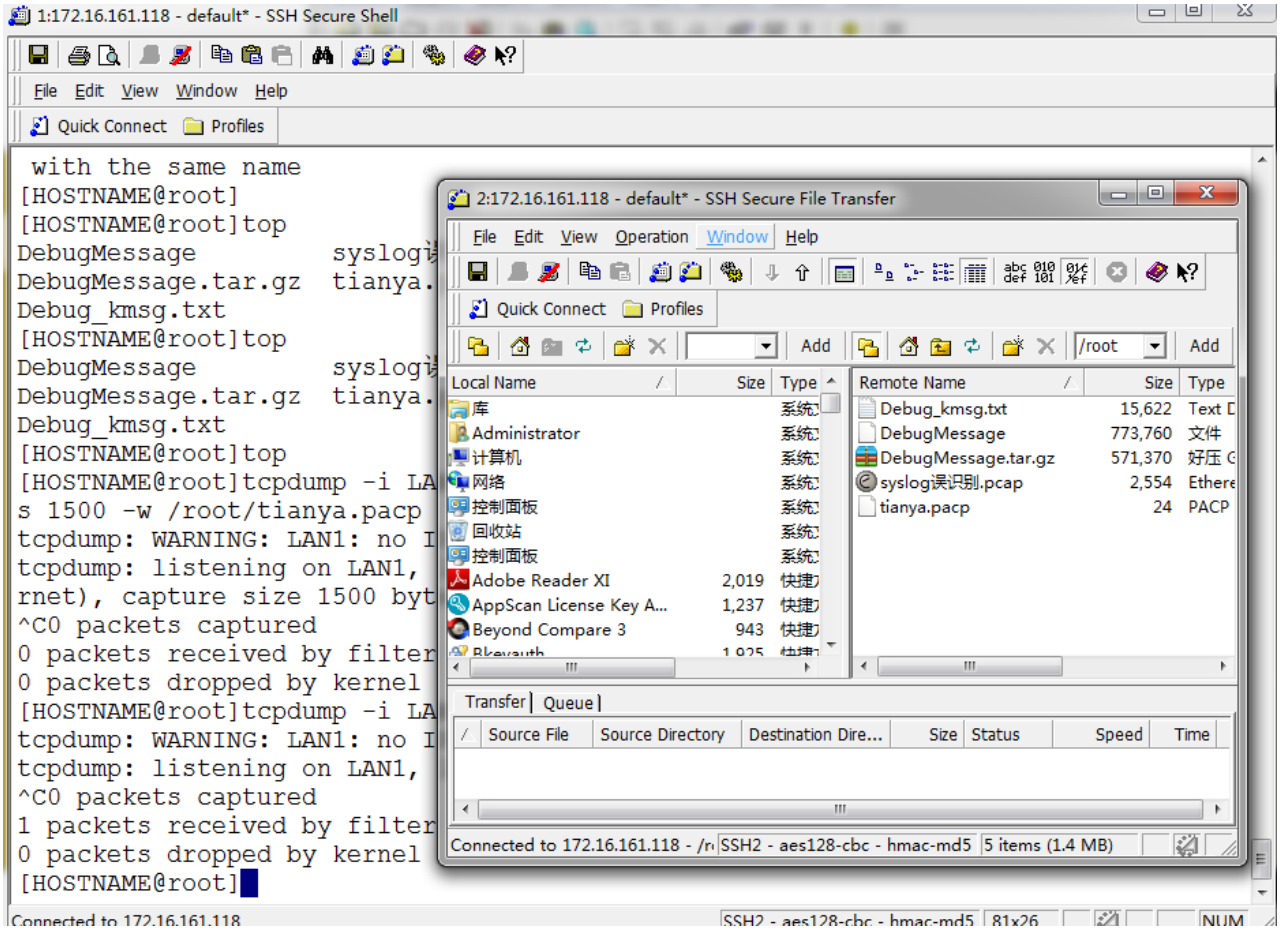
然后输入命令：tcpdump -i LAN1 host 172.16.1.122 -s 1500 -w /root/tianya.pacp

说明将开始抓取主机地址为 172.16.1.122 的数据报文，把抓取的数据包记录存到/root/tianya.pacp，当抓取 1500 个数据包后就退出程序



然后开始登录论坛，发帖，评论。结束之后，同时按 ctrl 和 c，就可以结束抓包。

2,如何下载已经抓到的包，



最后，把右边的包直接拖到左边电脑里保存即可。

7.2.3 系统重启

步骤

重启配置

```
# reboot
```