

<div>403 Forbidden</div> <div>本电子书由CyberArticle制作。点击<a href="#">这里</a>下载CyberArticle。注册版本不会显示该信息。<a href="#">删除广告</a></div>
<div>本电子书由CyberArticle制作。点击<a href="#">这里</a>下载CyberArticle。注册版本不会显示该信息。<a href="#">删除广告</a></div>
<div>本电子书由CyberArticle制作。点击<a href="#">这里</a>下<b>载</b>CyberArticle。注册版本不会显示该信息。<a href="#">删除广告</a></div>
<div>本电子书由CyberArticle制作。点击<a href="#">这里</a>下<b>载</b>CyberArticle。注册版本不会显示该信息。<a href="#">删除广告</a></div>
<div>本电子书由CyberArticle制作。点击<a href="#">这里</a>下<b>载</b>CyberArticle。注册版本不会显示该信息。<a href="#">删除广告</a></div>
<div>本电子书由CyberArticle制作。点击<a href="#">这里</a>下<b>载</b>CyberArticle。注册版本不会显示该信息。<a href="#">删除广告</a></div>
<div>本电子书由CyberArticle制作。点击<a href="#">这里</a>下<b>载</b>CyberArticle。注册版本不会显示该信息。<a href="#">删除广告</a></div>

# V5交换机作为SSH服务端登录配置方法

## 目录

- [V5交换机作为SSH服务端登录配置方法 1](#)
- [1 配置需求或说明 1](#)
  - [1.1适用产品系列 1](#)
  - [1.2配置需求 1](#)
- [2 组网图 1](#)
- [3 配置步骤 2](#)
  - [3.1 设备作为SSH服务器端设置 2](#)

### [3.2 SSH客户端设置以及配置验证 3](#)

## 1 配置需求或说明

### 1.1 适用产品系列

本案例适用于如S3100V2-16TP-EI、S5008PV2-EI、S5120-28P-SI、MS4120-26TP等的V5交换机，V5、V7交换机具体分类及型号可以参考“1.1 Comvare V5、V7平台交换机分类说明”。

### 1.2 配置需求

Host（SSH客户端）与Switch建立本地连接。Host采用SSH协议登录到Switch上，以保证数据信息交换的安全。此处采用的认证方式为password认证，用户名和密码保存在Switch上。

## 2 组网图



## 3 配置步骤

### 3.1 设备作为SSH服务器端设置

```
# 生成RSA密钥对。
<H3C>system-view
System View: return to User View with Ctrl+Z.
[H3C]public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
+++++
+++++
+++++
+++
# 生成DSA密钥对。
[H3C]public-key local create dsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
+++++
+++++*+++++

# 启动SSH服务器。
[H3C]ssh server enable
# 配置VLAN虚接口Vlan-interface 1的IP地址为192.168.1.1，此地址作为SSH服务器的登录地址。
[H3C]interface Vlan-interface 1
[H3C-Vlan-interface1] ip address 192.168.1.1 255.255.255.0
[H3C-Vlan-interface1]quit
```

```
# 设置SSH客户端登录用户界面的认证方式为scheme方式。
[H3C] user-interface vty 0 4
[H3C-ui-vty0-4] authentication-mode scheme
# 设置Switch上远程用户登录协议为SSH。
[H3C-ui-vty0-4] protocol inbound ssh
[H3C-ui-vty0-4] quit
# 创建本地用户client001，密码为aabbcc，并设置用户访问的命令级别为最高级别3。
[H3C] local-user client001
[H3C-luser-client001] password simple aabbcc
[H3C-luser-client001] service-type ssh
[H3C-luser-client001] authorization-attribute level 3
[H3C-luser-client001] quit
#保存配置
[H3C] save force
```

## 3.2 SSH客户端设置以及配置验证

SSH客户端软件有很多，此处以SecureCRT和PuTTY为例：

**SecureCRT登录方式如下：**

打开文件---快速连接，选择协议SSH1，输入设置的用户名和口令：

图1

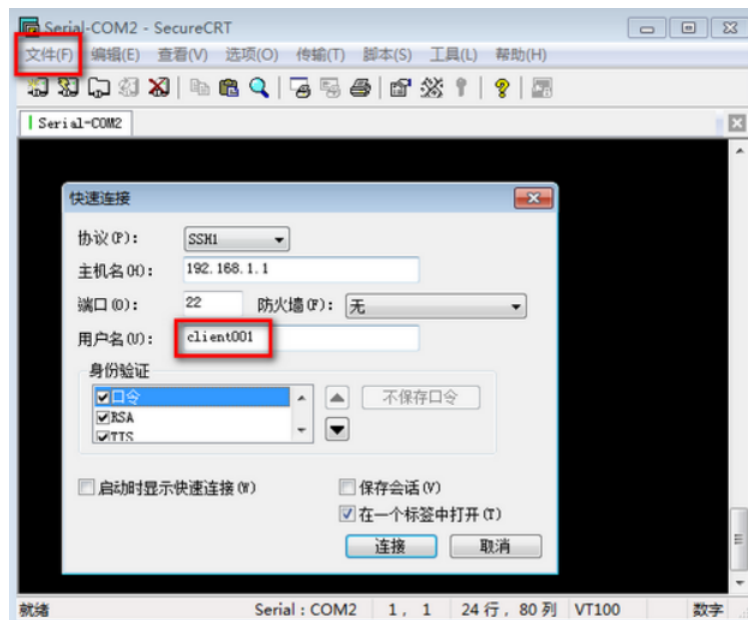


图2

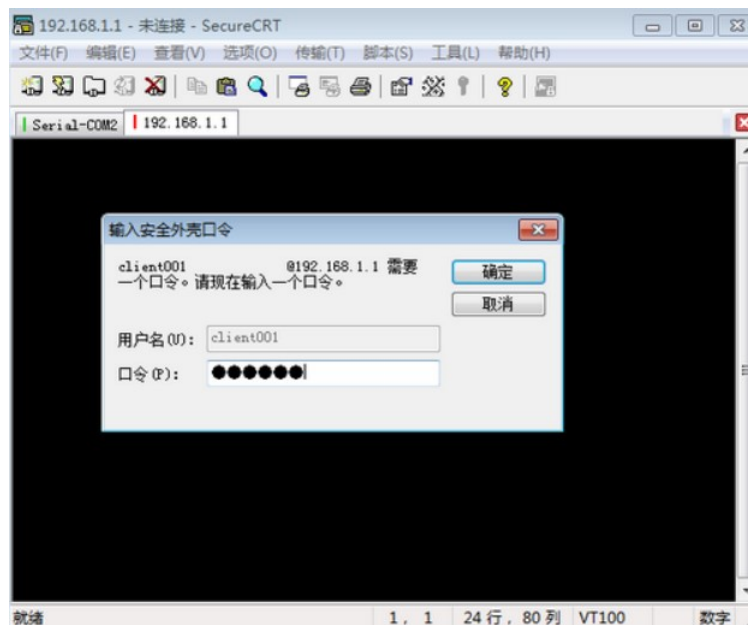
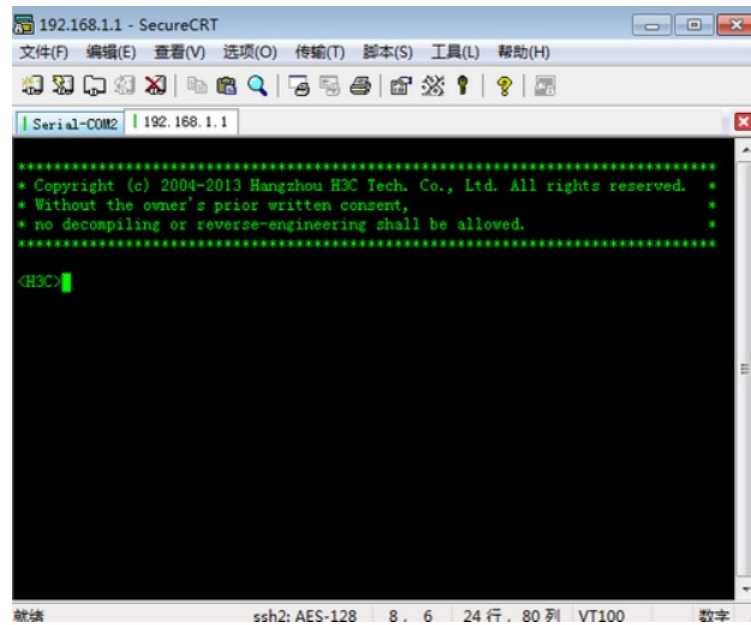


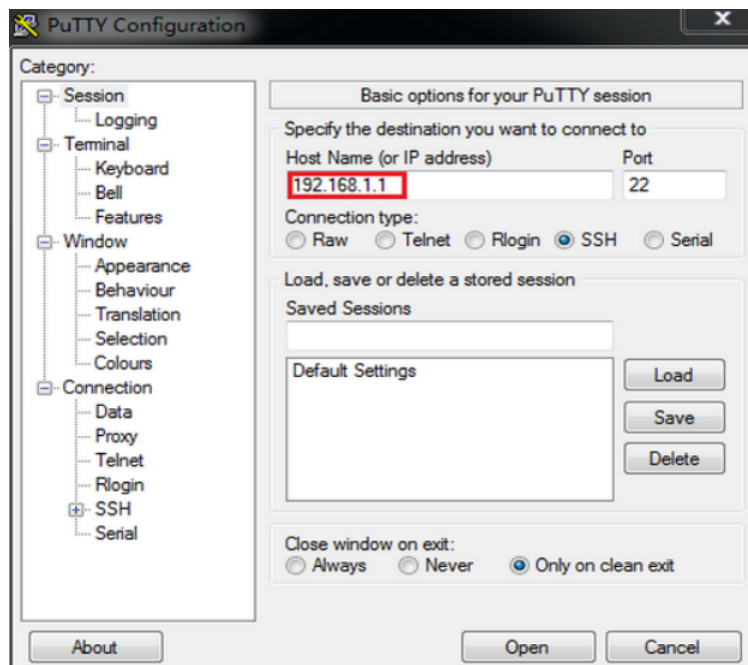
图3



登录成功

**使用PuTTY登录方式:**

打开 PuTTY.exe 程序, 出现如图所示的客户端配置界面。在 “Host Name (or IP address)” 文本框中输入SSH服务器的IP地址192.168.1.1。



单击<Open>按钮。按提示输入用户名client001及密码aabbcc，即可进入Switch的配置界面。