403 Forbidden
本电子书由CyberArticle制作。点击这里下载CyberArticle。注册版本不会显示该信息。 删除广告
本电子书由CyberArticle制作。点击这里下载CyberArticle。注册版本不会显示该信息。 删除广告
本电子书由CyberArticle制作。点击这里下载CyberArticle。注册版本不会显示该信息。 删除广告
本电子书由CyberArticle制作。点击这里下载CyberArticle。注册版本不会显示该信息。 删除广告
本电子书由CyberArticle制作。点击这里下载CyberArticle。注册版本不会显示该信息。 删除广告

V5 MSR路由器作为SSH服务端登录配置方法

目录

1 配置需求或说明

1.1适用产品系列

本案例适用于Comware V5 软件平台MSR WiNet系列路由器，如MSR830-WiNet 、MSR 830-10-WiNet 、MSR 930-WiNet 、MSR 930-10-WiNet 、MSR 930-WiNet-W 、MSR 2600-10-WiNet等。

1.2配置需求

Host（SSH客户端）与Router建立本地连接。Host采用SSH协议登录到Router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Router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password认证。

```
[H3C] user-interface vty 0 4
[H3C-ui-vty0-4]authentication-mode scheme
```

设置Router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
```

配置SSH用户client001的服务类型为Stelnet，认证方式为password认证（此步骤非必配）。

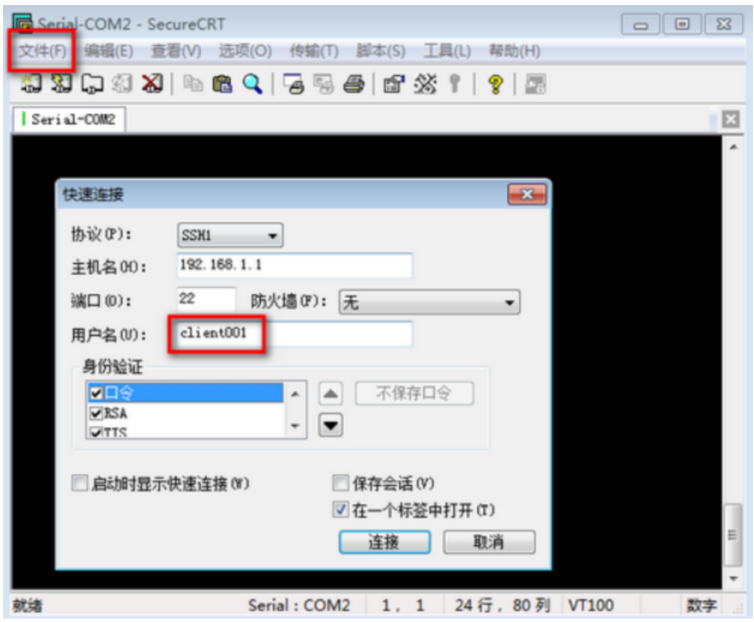
```
[H3C]ssh user client001 service-type stelnet authentication-
type password
```

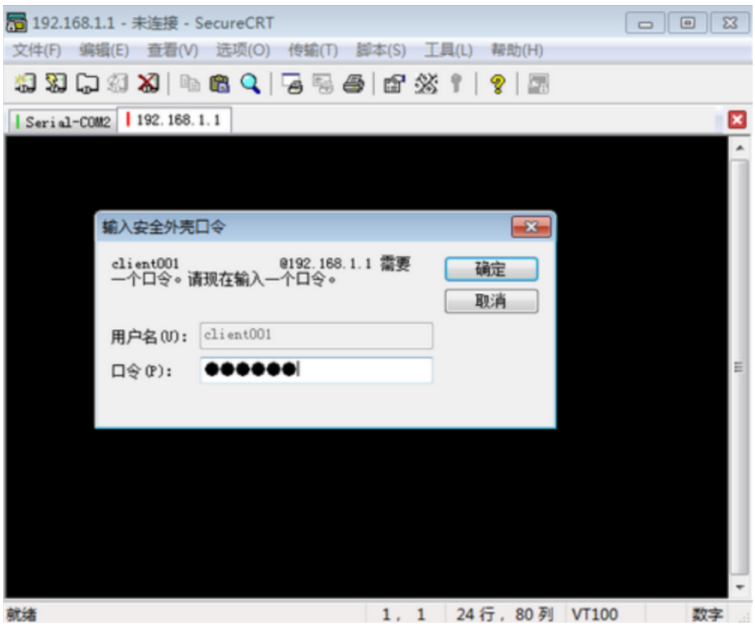
#保存配置

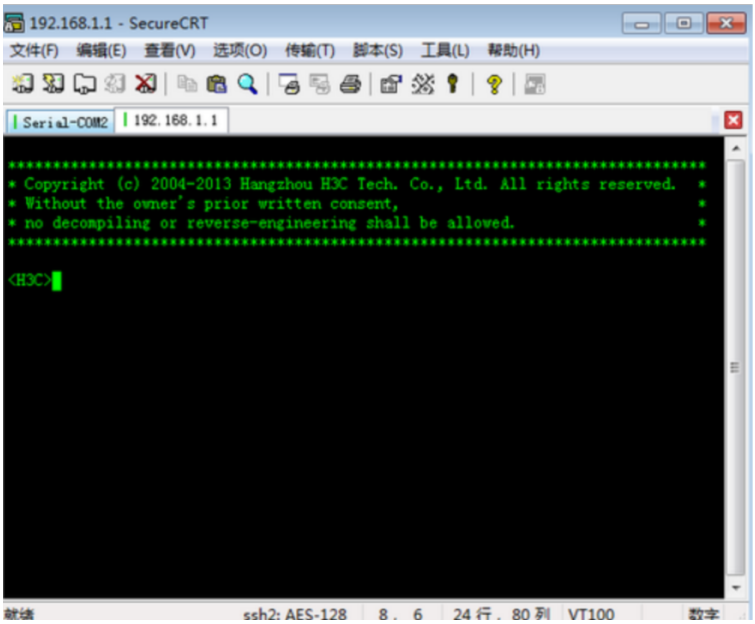
```
[H3C]save force
```

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为例：
打开文件---快速连接，选择协议SSH1，输入设置的用户名和口令：




192.168.1.1 - 未连接 - SecureCRT
文件(F) 编辑(E) 查看(V) 选项(O) 传输(T) 脚本(S) 工具(L) 帮助(H)
Serial-COM2
192.168.1.1
输入安全外壳口令
client001 @192.168.1.1 需要一个口令。请现在输入一个口令。
确定
取消
用户名(U): client001
口令(P):
就绪
1, 1
24 行, 80 列
VT100
数字


192.168.1.1 - SecureCRT
文件(F) 编辑(E) 查看(V) 选项(O) 传输(T) 脚本(S) 工具(L) 帮助(H)
Serial-COM2
192.168.1.1
* Copyright (c) 2004-2013 Hangzhou H3C Tech. Co., Ltd. All rights reserved. *
* Without the owner's prior written consent, *
* no decompiling or reverse-engineering shall be allowed. *
<H3C>
ssh2: AES-128 8, 6 24 行, 80 列 VT100