

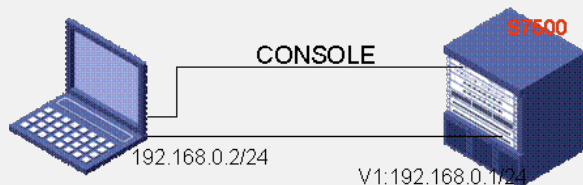
S7500交换机SSH功能的配置

一 组网需求：

如图1所示，PC终端（SSH Client）上运行支持SSH2.0的客户端软件，与交换机（SSH Server）建立本地连接，更大限度地保证数据信息交换的安全。

二 组网图：

如图1，配置PC的IP地址为192.168.0.2/24，交换机的vlan1虚接口地址为：192.168.0.1/24。



三 配置步骤：

1 生成本地RSA密钥。

```
<H3C>system-view
[H3C] rsa local-key-pair create
```

说明：

如果此前已完成生成本地密钥对的配置，可以略过此步操作。

2 设置用户登录认证方式。

下面按照两种认证方式分别进行配置。

第一种方式：password认证。

设置用户接口上的认证模式为AAA认证。

```
[H3C] user-interface vty 0 4
[H3C-ui-vty0-4] authentication-mode scheme
# 设置用户接口上支持SSH协议。
[H3C-ui-vty0-4] protocol inbound ssh
# 指定用户admin的登录协议为SSH，认证方式为password，认证密码为abc。
[H3C] local-user admin
[H3C-luser-admin] password simple abc
[H3C-luser-admin] service-type ssh
[H3C-luser-admin] quit
[H3C] ssh user admin authentication-type password
```

说明：

SSH的认证超时时间、重试次数可以采用系统默认值。完成以上配置后，用户就可以在与交换机连接的终端上，运行支持SSH2.0的客户端软件，以用户名admin，密码abc，访问交换机了。

第二种方式：RSA公钥认证。

设置用户接口上的认证模式为AAA认证。

```
[H3C] user-interface vty 0 4
[H3C-ui-vty0-4] authentication-mode scheme
# 设置用户接口上支持SSH协议。
[H3C-ui-vty0-4] protocol inbound ssh
# 指定用户client002的登录协议为SSH，认证方式为RSA公钥认证。
[H3C] ssh user client002 authentication-type rsa
# 在支持SSH2.0的客户端软件上，随机产生RSA密钥对，并将公钥部分传送到服务器端。
# 在服务器端配置客户端的公钥，指定公钥名称为huawei。
[H3C] rsa peer-public-key huawei
[H3C-rsa-public-key] public-key-code begin
[H3C-rsa-key-code] 308186028180739A291ABDA704F5D93DC8FDF84C427463
[H3C-rsa-key-code] 1991C164B0DF178C55FA833591C7D47D5381D09CE82913
[H3C-rsa-key-code] D7EDF9C08511D83CA4ED2B30B809808EB0D1F52D045DE4
[H3C-rsa-key-code] 0861B74A0E135523CCD74CAC61F8E58C452B2F3F2DA0DC
[H3C-rsa-key-code] C48E3306367FE187BDD944018B3B69F3CBB0A573202C16
```

```
[H3C-rsa-key-code] BB2FC1ACF3EC8F828D55A36F1CDDC4BB45504F020125
```

```
[H3C-rsa-key-code] public-key-code end
```

```
[H3C-rsa-public-key] peer-public-key end
```

```
[H3C] ssh user client002 assign rsa-key H3C002
```

说明：

服务器上配置的公钥是通过客户端上的SSH生成的。在目前的版本（313X系列）中，通过H3C公司自主开发的SSHkey.exe转换工具，将SSH客户端软件生成的公钥转换成交换机能够识别的格式。

3 配置SSH用户和客户端公钥的对应关系

用户admin和客户端公钥huawei相对应

即：使用admin认证的时候就会使用huawei这个公钥进行验证

```
[H3C]ssh user admin assign rsa-key huawei
```

4 配置SSH用户的服务类型

配置交换机SSH登陆的时候选择的服务类型

```
[H3C]ssh user admin service-type all
```

在保留有RSA私钥的终端上启动SSH客户端软件，并进行相应的配置，即可建立SSH连接。

四 配置关键点：

配置SSH用户的服务类型是必要的。

另外，建议使用Putty来生成公钥和私钥。交换机不能识别Putty生成的公钥，需要使用H3C公司的sshkey将公钥转换成交换机能识别的格式。后续的版本支持直接将putty生成的公钥上传到交换机的flash中，然后使用命令行进行转换成交换机能识别的格式。