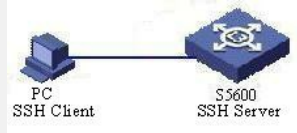


S5600系列交换机作为SSH Server的配置

一、组网需求:

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, 更最大限度地保证数据信息交换的安全。

二、组网图



三、配置步骤:

(1) 生成本地RSA密钥。

```
<Switch>system-view
```

```
[Switch] rsa local-key-pair create
```

//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。

```
[Switch] user-interface vty 0 4
```

```
[Switch-ui-vty0-4] authentication-mode scheme
```

设置用户接口上支持SSH协议。

```
[Switch-ui-vty0-4] protocol inbound ssh
```

指定用户client001的登录协议为SSH, 认证方式为password, 认证密码为abc。

```
[Switch] local-user client001
```

```
[Switch-luser-client001] password simple abc
```

```
[Switch-luser-client001] service-type ssh
```

```
[Switch-luser-client001] quit
```

```
[Switch] ssh user client001 authentication-type password
```

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。

```
[Switch] user-interface vty 0 4
```

```
[Switch-ui-vty0-4] authentication-mode scheme
```

设置用户接口上支持SSH协议。

```
[Switch-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。

```
[Switch] 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switch002。

```
[Switch] rsa peer-public-key switch002
```

```
[Switch-rsa-public-key] public-key-code begin
```

```
[Switch-rsa-key-code] 308186028180739A291ABDA704F5D93DC8FDF84C427463
```

```
[Switch-rsa-key-code] 1991C164B0DF178C55FA833591C7D47D5381D09CE82913
```

```
[Switch-rsa-key-code]
```

```
D7EDF9C08511D83CA4ED2B30B809808EB0D1F52D045DE4
```

```
[Switch-rsa-key-code]
```

```
0861B74A0E135523CCD74CAC61F8E58C452B2F3F2DA0DC
```

```
[Switch-rsa-key-code] C48E3306367FE187BDD944018B3B69F3CBB0A573202C16
```

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

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

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

```
[Switch] ssh user client002 assign rsa-key switch002
```

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:

1. 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client001，密码abc，访问交换机了。

2. Server端的public-key-code需要使用特定的软件生成并转换成S5600系列交换机支持的格式。此处使用puttygen.exe软件生成公钥并使用H3C公司提供的转换软件进行公钥转化。