S3500-EA系列交换机作为SSH服务器并采用publickey认证（认证密钥算法为RSA）功能的配置

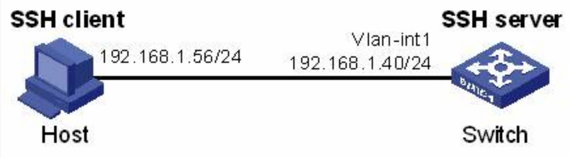
岳斌　2008-09-02 发表

S3500-EA系列交换机作为SSH服务器并采用publickey认证（认证密钥算法为RSA）功能的配置

一、　组网需求：

配置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。SSH用户采用的认证方式为publickey认证，认证时采用的公共密钥算法为RSA。

二、　组网图：



三、　配置步骤：

（1）配置SSH服务器Switch

# 生成RSA及DSA密钥对，并启动SSH服务器。

```
<Switch> system-view
[Switch] public-key local create rsa
[Switch] public-key local create dsa
[Switch] ssh server enable
```

# 配置VLAN接口1的IP地址，客户端将通过该地址连接SSH服务器。

```
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 192.168.1.40 255.255.255.0
[Switch-Vlan-interface1] quit
```

# 设置用户接口上认证模式为AAA认证。

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

# 设置Switch上远程用户登录协议为SSH。

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

# 设置用户能访问的命令级别为3。

```
[Switch-ui-vty0-4] user privilege level 3
[Switch-ui-vty0-4] quit
```

# 从文件key.pub中导入远端的公钥。

```
[Switch] public-key peer Switch001 import sshkey key.pub
```

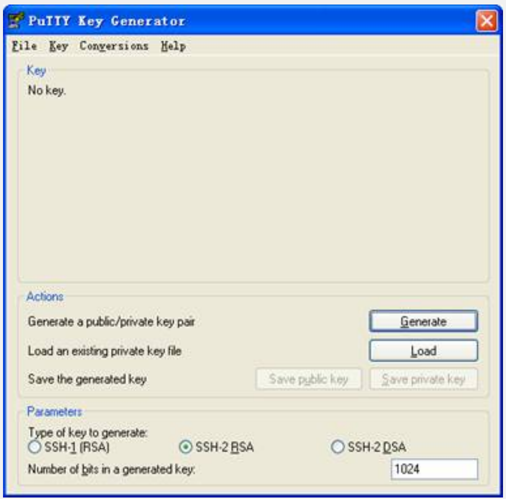
# 设置SSH用户client002的认证方式为publickey，并指定公钥为Switch001。

```
[Switch] ssh user client002 service-type stelnet authentication-type
publickey assign publickey Switch001
```

（2）配置SSH客户端Host

# 生成RSA密钥对。

在客户端运行PuTTYGen.exe，在参数栏中选择“SSH-2 RSA”，点击<Generate>，产生客户端密钥对。

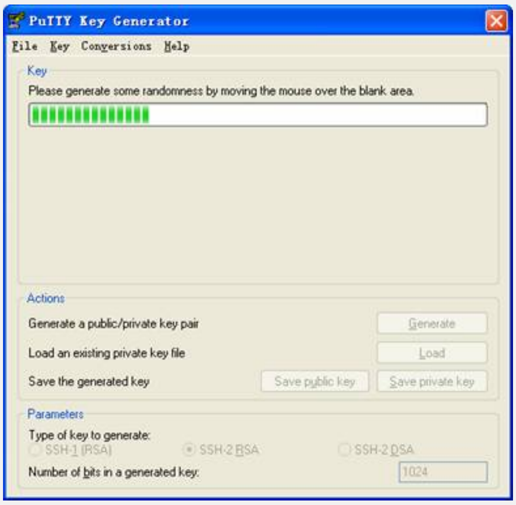


Key
No key.

Actions
Generate a public/private key pair
Load an existing private key file
Save the generated key

Parameters
Type of key to generate:
○ SSH-1 (RSA)　● SSH-2 RSA　○ SSH-2 DSA
Number of bits in a generated key: 1024

在产生密钥对的过程中需不停的移动鼠标，鼠标移动仅限于下图蓝色框中除绿色标记进程条外的地方，否则进程条的显示会不动，密钥对将停止产生。



Please generate some randomness by moving the mouse over the blank area.

Generate a public/private key pair

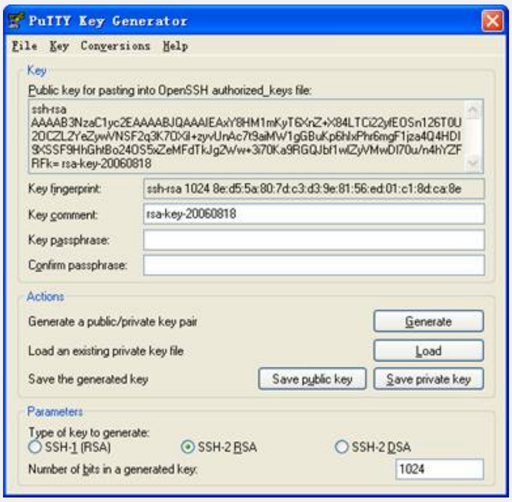
Load an existing private key file

Save the generated key

Type of key to generate:
○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 1024

密钥对产生后，点击<Save public key>，输入存储公钥的文件名key.pub，点击保存。



Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAIEAxY8HM1mKyT6XnZ+X84LTCi22yfEOSn126T0U
20CZL2YeZywVNSF2q3K70XiI+zyvUnAc7t9aiMW1gGBuKp6hlxPhr6mgF1jza4Q4HDI
9XSSF9HhGhtBo24OS5xZeMFdTkJg2Ww+3i70Ka9RGQJbf1wlZyVMwDI70u/n4hYZF
RFk= rsa-key-20060818
```

Key fingerprint: ssh-rsa 1024 8e:d5:5a:80:7d:c3:d3:9e:81:56:ed:01:c1:8d:ca:8e

Key comment: rsa-key-20060818

Key passphrase:

Confirm passphrase:

Generate a public/private key pair

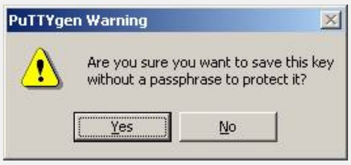
Load an existing private key file

Save the generated key

Type of key to generate:
○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

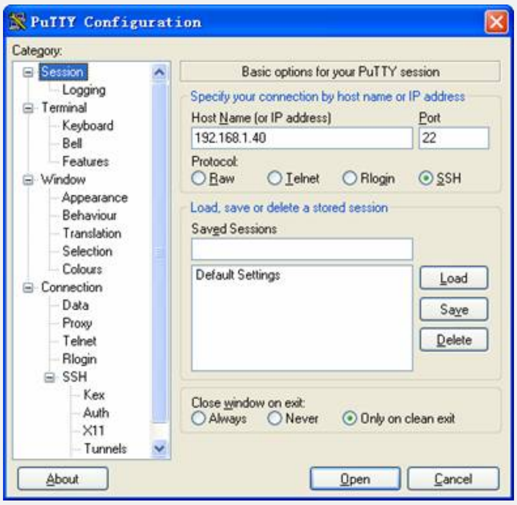
Number of bits in a generated key: 1024

点击<Save private key>存储私钥，弹出警告框，提醒是否保存没做任何保护措施的私钥，点击<Yes>，输入私钥文件名为private，点击保存。



Are you sure you want to save this key without a passphrase to protect it?

# 指定私钥文件，并建立与SSH服务器的连接。
打开PuTTY.exe程序，出现如下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地址为192.168.1.40。



Basic options for your PuTTY session

Specify your connection by host name or IP address

Host Name (or IP address): 192.168.1.40 Port: 22

Protocol: ○ Raw ○ Telnet ○ Rlogin ● SSH

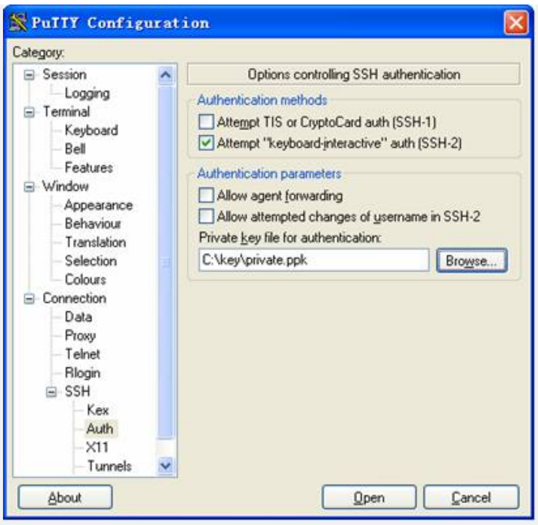
Load, save or delete a stored session

Saved Sessions

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

单击“SSH”下面的“Auth”（认证），出现如下图所示的界面。单击<Browse…>按钮，弹出文件选择窗口。选择与配置到服务器端的公钥对应的私钥文件private。



Options controlling SSH authentication

Authentication methods

□ Attempt TIS or CryptoCard auth (SSH-1)

☑ Attempt "keyboard-interactive" auth (SSH-2)

Authentication parameters

□ Allow agent forwarding

□ Allow attempted changes of username in SSH-2

Private key file for authentication:

C:\key\private.ppk

（3）之后，单击<Open>按钮，按提示输入用户名client002，即可进入Switch的配置界面。

四、 配置关键点:

（1）SSH客户端通过publickey和password两种方式进行认证尝试的次数总和，不能超过ssh server authentication-retries命令配置的SSH连接认证尝试次数，否则，客户端认证失败，无法登录SSH服务器。

（2）目前，设备作为SSH服务器时，支持SSH2和SSH1两个版本；设备作为SSH客户端时，只支持SSH2版本。

（3）S3500-EA系列以太网交换机的软件版本只支持RSA密钥对。