H3C 无线控制器

SSH 典型配置举例(V7)

资料版本：6W100-20191125

目 录

1 简介

本文档介绍 SSH 典型配置举例。

2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 WLAN 接入和 SSH 的特性。

3 设备作为Stelnet服务器配置举例（password认证）

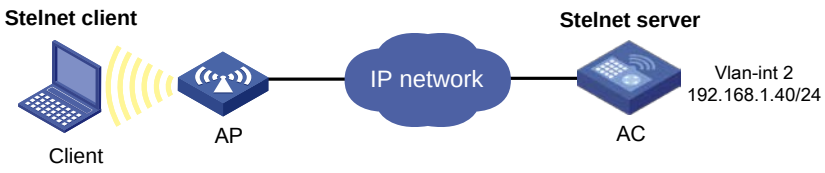
说明

无线控制器和客户端路由可达。

3.1 组网需求

- 用户可以通过 Client 上运行的 Stelnet 客户端软件（SSH2 版本）安全地登录到 AC 上，并被授予用户角色 network-admin 进行配置管理；
- AC 采用 password 认证方式对 Stelnet 客户端进行认证，客户端的用户名和密码保存在本地。

图1 设备作为 Stelnet 服务器配置组网图



3.2 配置步骤

(1) 配置 Stelnet 服务器

生成 RSA 密钥对。

```
<AC> system-view
[Switch] public-key local create rsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
```

```
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....................++++++
.................++++++
..++++++++
............++++++++
Create the key pair successfully.
```

生成 DSA 密钥对。

```
[AC] public-key local create dsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.................................+
...+.................+..........+...+.
Create the key pair successfully.
```

生成 ECDSA 密钥对。

```
[AC] public-key local create ecdsa secp256r1
Generating Keys...
.
Create the key pair successfully.
```

使能 Stelnet 服务器功能。

```
[AC] ssh server enable
```

配置 VLAN 接口 2 的 IP 地址，客户端将通过该地址连接 Stelnet 服务器。

```
[AC] interface vlan-interface 2
[AC-Vlan-interface2] ip address 192.168.1.40 255.255.255.0
[AC-Vlan-interface2] quit
```

设置 Stelnet 客户端登录用户线的认证方式为 AAA 认证。

```
[AC] line vty 0 15
[AC-line-vty0-15] authentication-mode scheme
[AC-line-vty0-15] quit
```

创建设备管理类本地用户 client001，并设置密码为明文 aabbcc，服务类型为 SSH，用户角色为 network-admin。

```
[AC] local-user client001 class manage
[AC-luser-manage-client001] password simple aabbcc
[AC-luser-manage-client001] service-type ssh
[AC-luser-manage-client001] authorization-attribute user-role network-admin
[AC-luser-manage-client001] quit
```

配置 SSH 用户 client001 的服务类型为 Stelnet，认证方式为 password 认证。（此步骤可以不配置）

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

3.3 验证配置

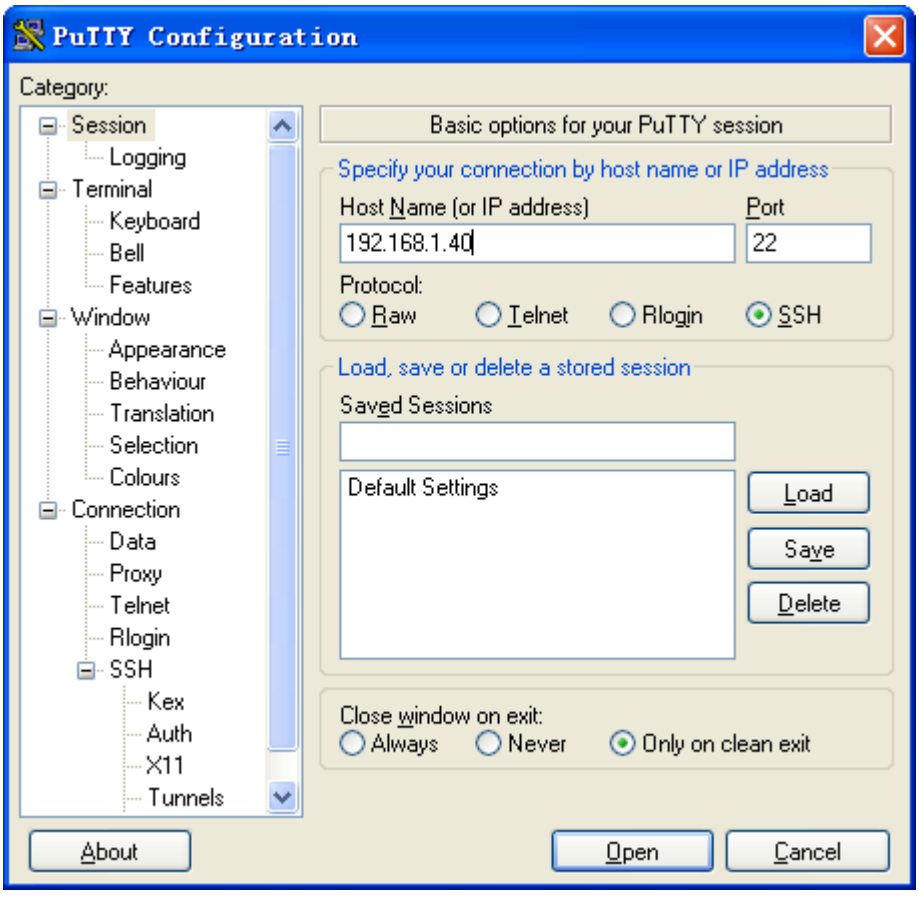
说明

Stelnet 客户端软件有很多，例如 PuTTY、OpenSSH 等。本文中仅以客户端软件 PuTTY0.58 为例，说明 Stelnet 客户端的配置方法。

建立与 Stelnet 服务器端的连接。

打开 PuTTY.exe 程序，出现如图 2 所示的客户端配置界面。在“Host Name（or IP address）”文本框中输入 Stelnet 服务器的 IP 地址为 192.168.1.40。

图2 Stelnet 客户端配置界面



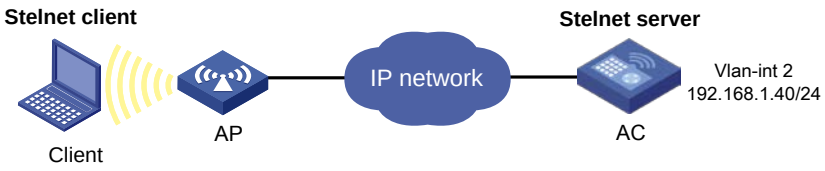
在图 2 中，单击<Open>按钮。按提示输入用户名 client001 及密码 aabbcc，即可进入 AC 的配置界面。

4 设备作为Stelnet服务器配置举例（publickey认证）

4.1 组网需求

- 用户可以通过 Client 上运行的 Stelnet 客户端软件（SSH2 版本）安全地登录到 AC 上，并被授予用户角色 network-admin 进行配置管理；
- AC 采用 publickey 认证方式对 Stelnet 客户端进行认证，使用的公钥算法为 RSA。

图3 设备作为 Stelnet 服务器配置组网图



4.2 配置步骤

说明

- 在服务器的配置过程中需要指定客户端的公钥信息，因此建议首先完成客户端密钥对的配置，再进行服务器的配置。
- 客户端软件有很多，例如 PuTTY、OpenSSH 等。本文中仅以客户端软件 PuTTY0.58 为例，说明 Stelnet 客户端的配置方法。

(1) 配置 Stelnet 客户端

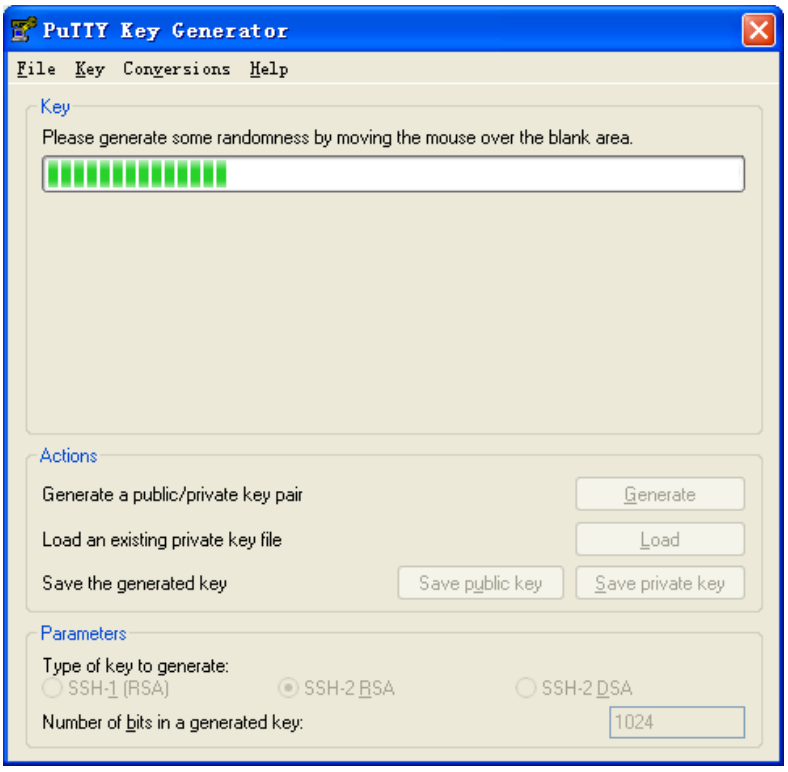
生成 RSA 密钥对。

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。

图4 生成客户端密钥（步骤 1）

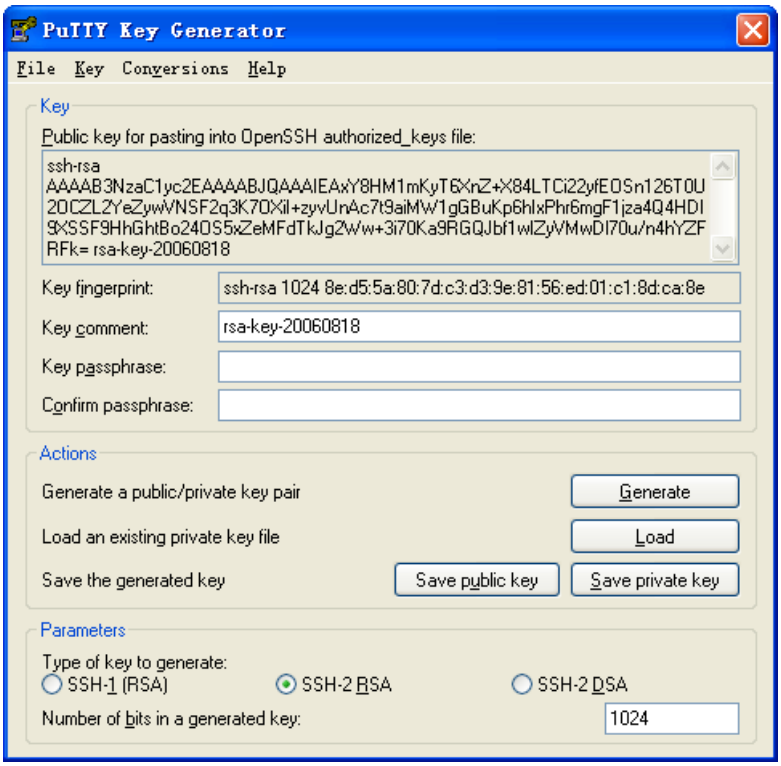
在产生密钥对的过程中需不停地移动鼠标，鼠标移动仅限于下图蓝色框中除绿色标记进程条外的地方，否则进程条的显示会不动，密钥对将停止产生，见图 5。

图5 生成客户端密钥（步骤 2）



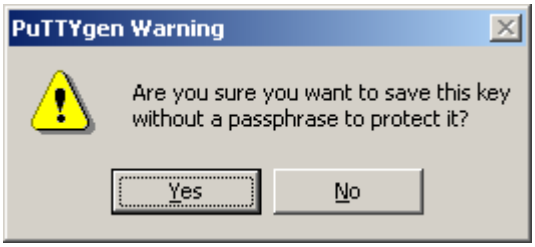
密钥对产生后，点击<Save public key>，输入存储公钥的文件名 key.pub，点击<保存>按钮。

图6 生成客户端密钥（步骤 3）



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.ppk，点击保存。

图7 生成客户端密钥（步骤 4）



客户端生成密钥对后，需要将保存的公钥文件 key.pub 通过 FTP/TFTP 方式上传到服务器，具体过程略。

(2) 配置 Stelnet 服务器

生成 RSA 密钥对。

```
<AC> system-view
[AC] public-key local create rsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
```

```
.......................++++++
..................++++++
..++++++++
............++++++++
Create the key pair successfully.
```

生成 DSA 密钥对。

```
[AC] public-key local create dsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.....................................+
...+.................+.........+...+
Create the key pair successfully.
```

生成 ECDSA 密钥对。

```
[AC] public-key local create ecdsa secp256r1
Generating Keys...
.
Create the key pair successfully.
```

使能 Stelnet 服务器功能。

```
[AC] ssh server enable
```

配置 VLAN 接口 2 的 IP 地址，客户端将通过该地址连接 Stelnet 服务器。

```
[AC] interface vlan-interface 2
[AC-Vlan-interface2] ip address 192.168.1.40 255.255.255.0
[AC-Vlan-interface2] quit
```

设置 Stelnet 客户端登录用户线的认证方式为 AAA 认证。

```
[AC] line vty 0 15
[AC-line-vty0-15] authentication-mode scheme
[AC-line-vty0-15] quit
```

从文件 key.pub 中导入远端的公钥，并命名为 ackey。

```
[AC] public-key peer ackey import sshkey key.pub
```

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

```
[AC] ssh user client002 service-type stelnet authentication-type publickey assign publickey
ackey
```

创建设备管理类本地用户 client002，并设置服务类型为 SSH，用户角色为 network-admin。

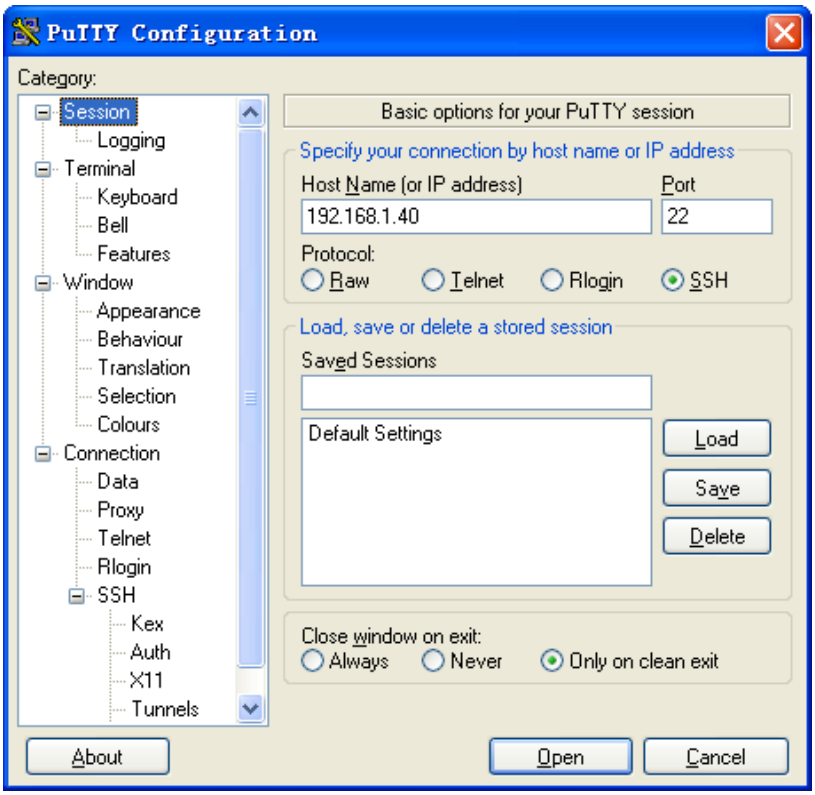
```
[AC] local-user client002 class manage
[AC-luser-manage-client002] service-type ssh
[AC-luser-manage-client002] authorization-attribute user-role network-admin
[AC-luser-manage-client002] quit
```

4.3 验证配置

指定私钥文件，并建立与 Stelnet 服务器的连接。

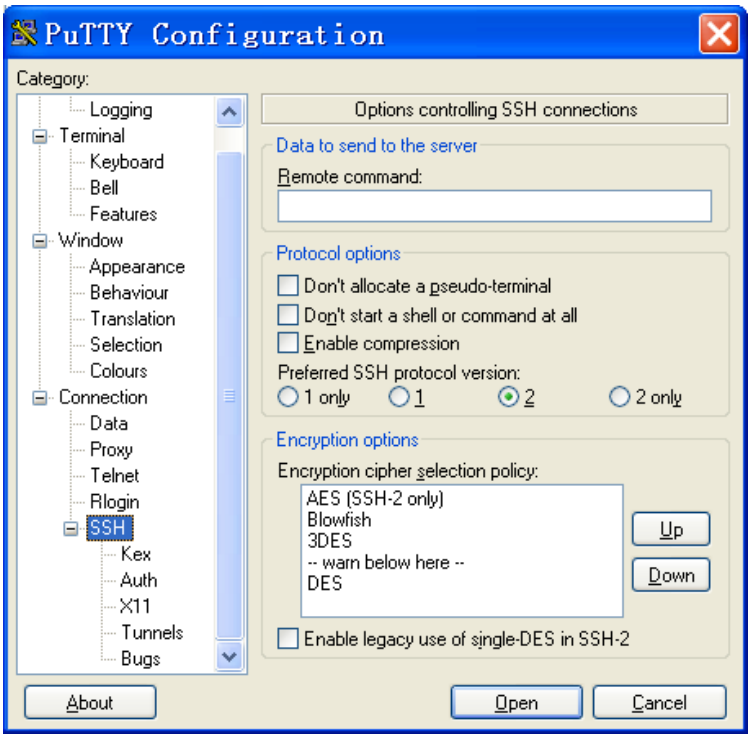
打开 PuTTY.exe 程序，出现如图 8 所示的客户端配置界面。在“Host Name（or IP address）”文本框中输入 Stelnet 服务器的 IP 地址为 192.168.1.40。

图8 Stelnet 客户端配置界面



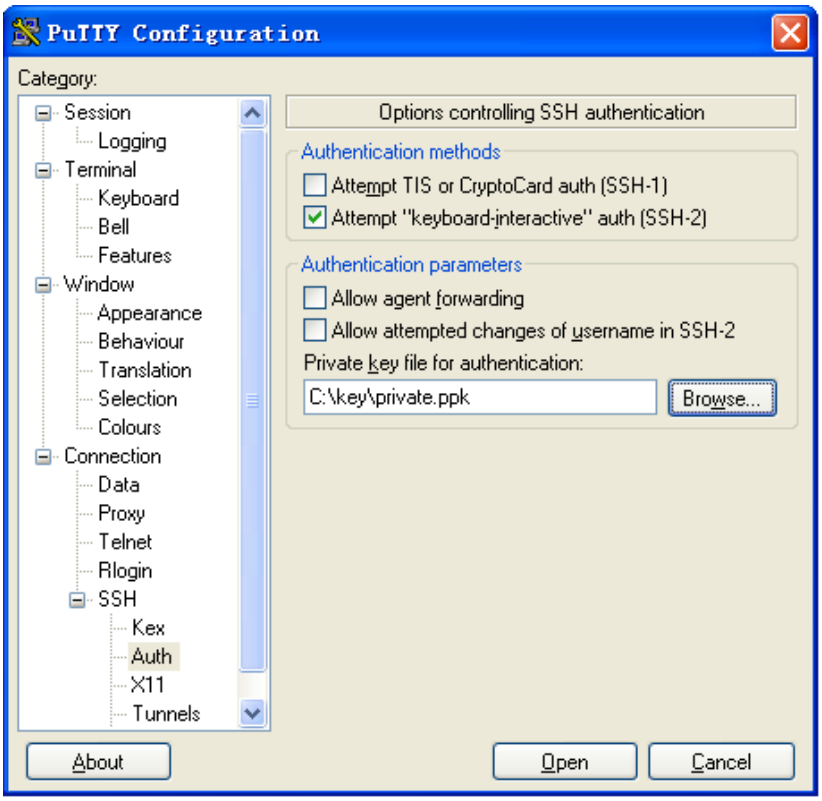
单击左侧导航栏“Connection->SSH”，出现如图 9 的界面。选择“Preferred SSH protocol version”为“2”。

图9 Stelnet 客户端配置界面



单击左侧导航栏“Connection->SSH”下面的“Auth”（认证），出现如图 10 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.ppk。

图10 Stelnet 客户端配置界面



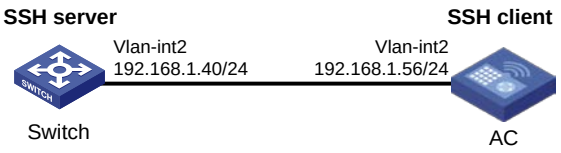
如图 10，单击<Open>按钮。按提示输入用户名 client002，即可进入 Switch 的配置界面。

5 设备作为Stelnet客户端配置举例（password认证）

5.1 组网需求

- 配置 AC 作为 Stelnet 客户端，用户能够通过 AC 安全地登录到 Switch 上，并被授予用户角色 network-admin 进行配置管理。
- Switch 作为 Stelnet 服务器采用 password 认证方式对 Stelnet 客户端进行认证，客户端的用户名和密码保存在 Switch 上。

图11 设备作为 Stelnet 客户端配置组网图



5.2 配置步骤

(1) 配置 Stelnet 服务器

生成 RSA 密钥对。

```
<Switch> system-view
[Switch] public-key local create rsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....................++++++
.................++++++
..++++++++
............++++++++
Create the key pair successfully.
```

生成 DSA 密钥对。

```
[Switch] public-key local create dsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.................................+
...+.................+..........+...+
Create the key pair successfully.
```

生成 ECDSA 密钥对。

```
[Switch] public-key local create ecdsa secp256r1
Generating Keys...
.
Create the key pair successfully.
```

使能 Stelnet 服务器功能。

```
[Switch] ssh server enable
```

配置 VLAN 接口 2 的 IP 地址，客户端将通过该地址连接 Stelnet 服务器。

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.1.40 255.255.255.0
[Switch-Vlan-interface2] quit
```

设置 Stelnet 客户端登录用户线的认证方式为 AAA 认证。

```
[Switch] line vty 0 15
[Switch-line-vty0-15] authentication-mode scheme
[Switch-line-vty0-15] quit
```

创建设备管理类本地用户 client001，并设置密码为明文 aabbcc，服务类型为 SSH，用户角色为 network-admin。

```
[Switch] local-user client001 class manage
[Switch-luser-manage-client001] password simple aabbcc
[Switch-luser-manage-client001] service-type ssh
[Switch-luser-manage-client001] authorization-attribute user-role network-admin
[Switch-luser-manage-client001] quit
```

配置 SSH 用户 client001 的服务类型为 Stelnet，认证方式为 password 认证。（此步骤可以不配置）

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

(2) Stelnet 客户端建立与 Stelnet 服务器的连接

配置 VLAN 接口 2 的 IP 地址。

```
<AC> system-view
[AC] interface vlan-interface 2
[AC-Vlan-interface2] ip address 192.168.1.56 255.255.255.0
[AC-Vlan-interface2] quit
[AC] quit
```

5.3 验证配置

- 客户端本地没有服务器端的主机公钥，首次与服务器建立连接

建立到服务器 192.168.1.40 的 SSH 连接，选择在不认证服务器的情况下继续访问服务网，并在客户端保存服务器端的本地公钥。

```
<AC> ssh2 192.168.1.40
Username: client001
Press CTRL+C to abort.
Connecting to 192.168.1.40 port 22.
The server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:y
client001@192.168.1.40's password:

Enter a character ~ and a dot to abort.

************************************************************************
* Copyright (c) 2004-2019 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                           *
* no decompiling or reverse-engineering shall be allowed.              *
************************************************************************

<Switch>
```

输入正确的用户名和密码之后，即可成功登录到 Switch 上。由于选择在本地保存服务器端的主机公钥，下次用户登录 Switch 时直接输入正确密码即可成功登录。

- 客户端配置服务器端的主机公钥后，与服务器建立连接

在客户端配置 SSH 服务器端的主机公钥。在公钥视图输入服务器端的主机公钥，即在服务器端通过 **display public-key local dsa public** 命令显示的公钥内容。

```
[AC] public-key peer key1
Enter public key view. Return to system view with "peer-public-key end" command.
[AC-pkey-public-key-key1]308201B73082012C06072A8648CE3804013082011F0281810
0D757262C4584C44C211F18BD96E5F0
[AC-pkey-public-key-key1]61C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE
65BE6C265854889DC1EDBD13EC8B274
[AC-pkey-public-key-key1]DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B0
6FD60FE01941DDD77FE6B12893DA76E
```

```
[AC-pkey-public-key-key1]EBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B3
68950387811C7DA33021500C773218C
[AC-pkey-public-key-key1]737EC8EE993B4F2DED30F48EDACE915F0281810082269009E
14EC474BAF2932E69D3B1F18517AD95
[AC-pkey-public-key-key1]94184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD35D02
492B3959EC6499625BC4FA5082E22C5
[AC-pkey-public-key-key1]B374E16DD00132CE71B020217091AC717B612391C76C1FB2E
88317C1BD8171D41ECB83E210C03CC9
[AC-pkey-public-key-key1]B32E810561C21621C73D6DAAC028F4B1585DA7F42519718CC
9B09EEF0381840002818000AF995917
[AC-pkey-public-key-key1]E1E570A3F6B1C2411948B3B4FFA256699B3BF871221CC9C5D
F257523777D033BEE77FC378145F2AD
[AC-pkey-public-key-key1]D716D7DB9FCABB4ADBF6FB4FDB0CA25C761B308EF53009F71
01F7C62621216D5A572C379A32AC290
[AC-pkey-public-key-key1]E55B394A217DA38B65B77F0185C8DB8095522D1EF044B465E
8716261214A5A3B493E866991113B2D
[AC-pkey-public-key-key1]485348
[AC-pkey-public-key-key1] peer-public-key end
[AC] quit
```

建立到服务器 192.168.1.40 的 SSH 连接，并指定服务器端的主机公钥。

```
<AC> ssh2 192.168.1.40 public-key key1
Username: client001
Press CTRL+C to abort.
Connecting to 192.168.1.40 port 22.
client001@192.168.1.40's password:
Enter a character ~ and a dot to abort.

******************************************************************************
* Copyright (c) 2004-2019 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

<Switch>
```

输入正确的用户名和密码之后，即可成功登录到 Switch B 上。

- 客户端本地已有服务器端的主机公钥，直接与服务器建立连接

```
<AC> ssh2 192.168.1.40
Username: client001
Press CTRL+C to abort.
Connecting to 192.168.1.40 port 22.
client001@192.168.1.40's password:
Enter a character ~ and a dot to abort.

******************************************************************************
* Copyright (c) 2004-2019 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************
```

```
<Switch>
```

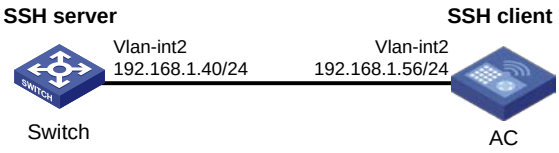
输入正确的密码之后，即可成功登录到 Switch B 上。

6 设备作为Stelnet客户端配置举例（publickey认证）

6.1 组网需求

- 配置 AC 作为 Stelnet 客户端，用户能够通过 AC 安全地登录到 Switch 上，并被授予用户角色 network-admin 进行配置管理。
- Switch 作为 Stelnet 服务器采用 publickey 认证方式对 Stelnet 客户端进行认证，使用的公钥算法为 DSA。

图12 设备作为 Stelnet 客户端配置组网图



6.2 配置步骤

说明

在服务器的配置过程中需要指定客户端的公钥信息，因此需要首先完成客户端密钥对的配置，再进行服务器的配置。

(1) 配置 Stelnet 客户端

配置 VLAN 接口 2 的 IP 地址。

```
<AC> system-view
[AC] interface vlan-interface 2
[AC-Vlan-interface2] ip address 192.168.1.56 255.255.255.0
[AC-Vlan-interface2] quit
```

生成 DSA 密钥对。

```
[AC] public-key local create dsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.....................................+
...+.................+..........+...+
Create the key pair successfully.
```

将生成的 DSA 主机公钥导出到指定文件 key.pub 中。

```
[AC] public-key local export dsa ssh2 key.pub
[AC] quit
```

客户端生成密钥对后，需要将保存的公钥文件 key.pub 通过 FTP/TFTP 方式上传到服务器，具体过程略。

(2) 配置 Stelnet 服务器

生成 RSA 密钥对。

```
<Switch> system-view
[Switch] public-key local create rsa
The range of public key size is (512 ~ 2048)
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....................++++++
.................++++++
..++++++++
............++++++++
Create the key pair successfully.
```

生成 DSA 密钥对。

```
[Switch] public-key local create dsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.....................................+
...+.................+..........+...+
Create the key pair successfully.
```

生成 ECDSA 密钥对。

```
[Switch] public-key local create ecdsa secp256r1
Generating Keys...
.
Create the key pair successfully.
```

使能 Stelnet 服务器功能。

```
[Switch] ssh server enable
```

配置 VLAN 接口 2 的 IP 地址，客户端将通过该地址连接 SSH 服务器。

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.1.40 255.255.255.0
[Switch-Vlan-interface2] quit
```

设置 Stelnet 客户端登录用户线的认证方式为 AAA 认证。

```
[Switch] line vty 0 15
[Switch-line-vty0-15] authentication-mode scheme
[Switch-line-vty0-15] quit
```

从文件 key.pub 中导入远端的公钥，并命名为 ackey。

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

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

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

创建设备管理类本地用户 client002，并设置服务类型为 SSH，用户角色为 network-admin。

```
[Switch] local-user client002 class manage
[Switch-luser-manage-client002] service-type ssh
[Switch-luser-manage-client002] authorization-attribute user-role network-admin
[Switch-luser-manage-client002] quit
```

6.3 验证配置

建立到服务器 192.168.1.40 的 SSH 连接。

```
<AC> ssh2 192.168.1.40
Username: client002
Press CTRL+C to abort.
Connecting to 192.168.1.40 port 22.
The server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
Enter a character ~ and a dot to abort.

******************************************************************************
* Copyright (c) 2004-2019 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

<Switch>
```

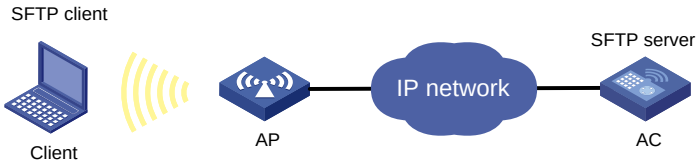
由于本地未保存服务器端的主机公钥，因此在选择继续访问服务器之后，即可成功登录到 Switch B 上。

7 设备作为SFTP服务器配置举例（password认证）

7.1 组网需求

- Client 和 AC 之间建立 SSH 连接，Client 作为 SFTP 客户端登录到 AC，，并被授予用户角色 network-admin 进行文件管理和文件传送等操作；
- AC 采用 password 认证方式对 SFTP 客户端进行认证，客户端的用户名和密码保存在本地。
- AC 和 Client 之间路由可达。

图13 设备作为 SFTP 服务器配置组网图



7.2 配置步骤

(1) 配置 SFTP 服务器

生成 RSA 密钥对。

```
<AC> system-view
[AC] public-key local create rsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.........................++++++
...................++++++
..++++++++
............++++++++
Create the key pair successfully.
```

生成 DSA 密钥对。

```
[AC] public-key local create dsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.....................................+
...+.................+..........+...+
Create the key pair successfully.
```

生成 ECDSA 密钥对。

```
[AC] public-key local create ecdsa secp256r1
Generating Keys...
.
Create the key pair successfully.
```

启动 SFTP 服务器。

```
[AC] sftp server enable
```

配置 VLAN 接口 2 的 IP 地址，客户端将通过该地址连接 SSH 服务器。

```
[AC] interface vlan-interface 2
[AC-Vlan-interface2] ip address 192.168.1.45 255.255.255.0
```

```
[AC-Vlan-interface2] quit
```

创建设备管理类本地用户 client002，并设置密码为明文 aabbcc，服务类型为 SSH，用户角色为 network-admin，工作目录为 cfa0:/。

```
[AC] local-user client002 class manage
[AC-luser-manage-client002] password simple aabbcc
[AC-luser-manage-client002] service-type ssh
[AC-luser-manage-client002] authorization-attribute user-role network-admin work-directory cfa0:/
[AC-luser-manage-client002] quit
```

配置 SSH 用户认证方式为 password，服务类型为 SFTP。（此步骤可以不配置）

```
[AC] ssh user client002 service-type sftp authentication-type password
```

7.3 验证配置

说明

- SFTP 客户端软件有很多，本文中仅以客户端软件 PuTTY0.58 中的 PSFTP 为例，说明 SFTP 客户端的配置方法。
- PSFTP 只支持 password 认证，不支持 publickey 认证。

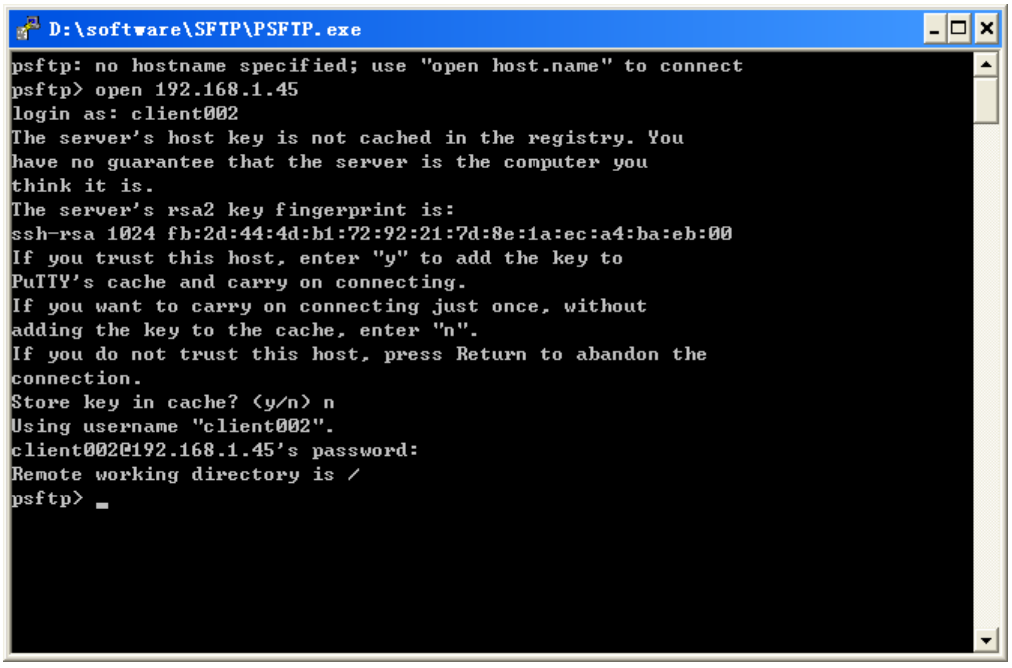
建立与 SFTP 服务器的连接。

打开 psftp.exe 程序，出现如图 14 所示的客户端配置界面。输入如下命令：

```
open 192.168.1.45
```

根据提示输入用户名 client002，密码 aabbcc，即可登录 SFTP 服务器。

图14 SFTP 客户端登录界面

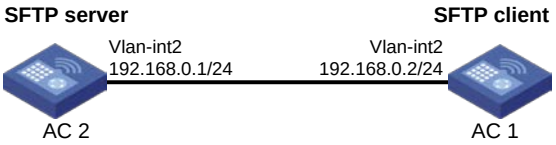


8 设备作为SFTP客户端配置举例（publickey认证）

8.1 组网需求

- 配置 AC 1 作为 SFTP 客户端，用户能够通过 AC 1 安全地登录到 AC 2 上，并被授予用户角色 network-admin 进行文件管理和文件传送等操作。
- AC 2 作为 SFTP 服务器采用 publickey 认证方式对 SFTP 客户端进行认证，使用的公钥算法为 RSA。

图15 设备作为 SFTP 客户端配置组网图



8.2 配置步骤

说明

在服务器的配置过程中需要指定客户端的公钥信息，因此建议首先完成客户端密钥对的配置，再进行服务器的配置。

(1) 配置 SFTP 客户端

配置 VLAN 接口 2 的 IP 地址。

```
<AC1> system-view
[AC1] interface vlan-interface 2
[AC1-Vlan-interface2] ip address 192.168.0.2 255.255.255.0
[AC1-Vlan-interface2] quit
```

生成 RSA 密钥对。

```
[AC1] public-key local create rsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....................++++++
.................++++++
..++++++++
............++++++++
Create the key pair successfully.
```

将生成的 RSA 主机公钥导出到指定文件 pubkey 中。

```
[AC1] public-key local export rsa ssh2 pubkey
[AC1] quit
```

客户端生成密钥对后，需要将保存的公钥文件 pubkey 通过 FTP/TFTP 方式上传到服务器，具体过程略。

(2) 配置 SFTP 服务器

生成 RSA 密钥对。

```
<AC2> system-view
[AC2] public-key local create rsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....................++++++
.................++++++
..++++++++
............++++++++
Create the key pair successfully.
```

生成 DSA 密钥对。

```
[AC2] public-key local create dsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.................................+
...+.................+.........+...+
Create the key pair successfully.
```

生成 ECDSA 密钥对。

```
[AC2] public-key local create ecdsa secp256r1
Generating Keys...
.
Create the key pair successfully.
```

启动 SFTP 服务器。

```
[AC2] sftp server enable
```

配置 VLAN 接口 2 的 IP 地址，客户端将通过该地址连接 SSH 服务器。

```
[AC2] interface vlan-interface 2
[AC2-Vlan-interface2] ip address 192.168.0.1 255.255.255.0
[AC2-Vlan-interface2] quit
```

从文件 pubkey 中导入远端的公钥，并命名为 ackey。

```
[AC2] public-key peer ackey import sshkey pubkey
```

设置 SSH 用户 client001 的服务类型为 SFTP，认证方式为 publickey，并指定公钥为 ackey。

```
[AC2] ssh user client001 service-type sftp authentication-type publickey assign publickey
ackey
```

创建设备管理类本地用户 client001，并设置服务类型为 SSH，用户角色为 network-admin，工作目录为 cfa0:/。

```
[AC2] local-user client001 class manage
```

```
[AC2-luser-manage-client001] service-type ssh
[AC2-luser-manage-client001] authorization-attribute user-role network-admin
work-directory cfa0:/
[AC2-luser-manage-client001] quit
```

8.3 验证配置

与远程 SFTP 服务器建立连接，进入 SFTP 客户端视图。

```
<AC1> sftp 192.168.0.1 identity-key rsa
Username: client001
Press CTRL+C to abort.
Connecting to 192.168.0.1 port 22.
The server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
sftp>
```

显示服务器的当前目录，删除文件 z，并检查此文件是否删除成功。

```
sftp> dir -l
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
-rwxrwxrwx   1 noone    nogroup       225 Sep 01 06:55 pub
-rwxrwxrwx   1 noone    nogroup         0 Sep 01 08:00 z
sftp> delete z
Removing /z
sftp> dir -l
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
-rwxrwxrwx   1 noone    nogroup       225 Sep 01 06:55 pub
```

新增目录 new1，并检查新目录是否创建成功。

```
sftp> mkdir new1
sftp> dir -l
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
-rwxrwxrwx   1 noone    nogroup       225 Sep 01 06:55 pub
drwxrwxrwx   1 noone    nogroup         0 Sep 02 06:30 new1
```

将目录名 new1 更名为 new2，并查看是否更名成功。

```
sftp> rename new1 new2
sftp> dir -l
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
-rwxrwxrwx   1 noone    nogroup       225 Sep 01 06:55 pub
```

```
drwxrwxrwx   1 noone    nogroup          0 Sep 02 06:33 new2
```

从服务器上下载文件 pubkey2 到本地，并更名为 public。

```
sftp> get pubkey2 public
Fetching / pubkey2 to public
/pubkey2                                      100% 225     1.4KB/s   00:00
```

将本地文件 pu 上传到服务器上，更名为 puk，并查看上传是否成功。

```
sftp> put pu puk
Uploading pu to / puk
sftp> dir -l
-rwxrwxrwx   1 noone    nogroup       1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup        225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup        283 Aug 24 07:39 pubkey
drwxrwxrwx   1 noone    nogroup          0 Sep 01 06:22 new
drwxrwxrwx   1 noone    nogroup          0 Sep 02 06:33 new2
-rwxrwxrwx   1 noone    nogroup        283 Sep 02 06:35 pub
-rwxrwxrwx   1 noone    nogroup        283 Sep 02 06:36 puk
sftp>
```

退出 SFTP 客户端视图。

```
sftp> quit
<AC1>
```

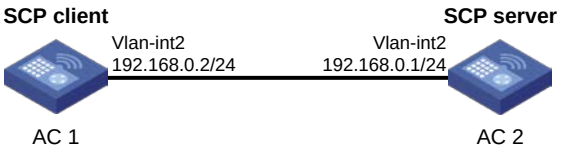
9 SCP文件传输配置举例（password认证）

9.1 组网需求

如下图所示，AC 1 作为 SCP 客户端，AC 2 作为 SCP 服务器。现有如下具体需求：

- 用户能够通过 AC 1 安全地安全地登录到 AC 2 上，并被授予用户角色 network-admin 与 AC 2 进行文件传输。
- AC 2 采用 password 认证对 SCP 客户端进行认证，客户端的用户名和密码保存在 AC 2 上。

图16 SCP 文件传输配置组网图



9.2 配置步骤

(1) 配置 SCP 服务器

生成 RSA 密钥对。

```
<AC2> system-view
[AC2] public-key local create rsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
```

```
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....................++++++
.................++++++
..++++++++
............++++++++
Create the key pair successfully.
```

生成 DSA 密钥对。

```
[AC2] public-key local create dsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.................................+
...+.................+.........+...+.
Create the key pair successfully.
```

生成 ECDSA 密钥对。

```
[AC2] public-key local create ecdsa secp256r1
Generating Keys...
.
Create the key pair successfully.
```

使能 SCP 服务器功能。

```
[AC2] scp server enable
```

配置接口 VLAN 接口 2 的 IP 地址，客户端将通过该地址连接 SCP 服务器。

```
[AC2] interface vlan-interface 2
[AC2-Vlan-interface2] ip address 192.168.0.1 255.255.255.0
[AC2-Vlan-interface2] quit
```

创建设备管理类本地用户 client001，并设置密码为明文 aabbcc，服务类型为 SSH。

```
[AC2] local-user client001 class manage
[AC2-luser-manage-client001] password simple aabbcc
[AC2-luser-manage-client001] service-type ssh
[AC2-luser-manage-client001] authorization-attribute user-role network-admin
[AC2-luser-manage-client001] quit
```

配置 SSH 用户 client001 的服务类型为 scp，认证方式为 password 认证。（此步骤可以不配置）

```
[AC2] ssh user client001 service-type scp authentication-type password
```

(2) 配置 SCP 客户端

配置接口 VLAN 2 的 IP 地址。

```
<AC1> system-view
[AC1] interface vlan-interface 2
[AC1-Vlan-interface2] ip address 192.168.0.2 255.255.255.0
[AC1-Vlan-interface2] quit
[AC1] quit
```

9.3 验证配置

与远程 SCP 服务器建立连接，并下载远端的 remote.bin 文件，下载到本地后更名为 local.bin。

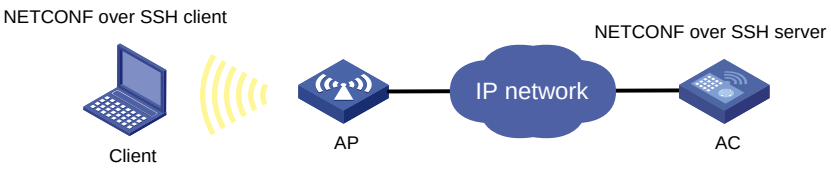
```
<AC1> scp 192.168.0.1 get remote.bin local.bin
Username: client001
Press CTRL+C to abort.
Connecting to 192.168.0.1 port 22.
The server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
client001@192.168.0.1's password:
remote.bin                                          100% 2875     2.8KB/s   00:00
```

10 NETCONF over SSH配置举例（password认证）

10.1 组网需求

- 用户可以通过 Client 上运行的支持 NETCONF over SSH 连接的 SSH 客户端软件（SSH2 版本）安全地登录到 AC 上，并被授予用户角色 network-admin 进行配置管理；
- AC 采用 password 认证方式对 Stelnet 客户端进行认证，客户端的用户名和密码保存在本地。
- AC 和 Client 之间路由可达。

图17 设备作为 NETCONF over SSH 服务器配置组网图



10.2 配置步骤

生成 RSA 密钥对。

```
<AC> system-view
[AC] public-key local create rsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....................++++++
.................++++++
..++++++++
............++++++++
Create the key pair successfully.
```

生成 DSA 密钥对。

```
[AC] public-key local create dsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.....................................+
...+.................+.........+...+.
Create the key pair successfully.
```

生成 ECDSA 密钥对。

```
[AC] public-key local create ecdsa secp256r1
Generating Keys...
.
Create the key pair successfully.
```

使能 NETCONF over SSH 服务器功能。

```
[AC] netconf ssh server enable
```

配置 VLAN 接口 2 的 IP 地址，客户端将通过该地址连接 NETCONF over SSH 服务器。

```
[AC] interface vlan-interface 2
[AC-Vlan-interface2] ip address 192.168.100.49 255.255.255.0
[AC-Vlan-interface2] quit
```

设置 NETCONF over SSH 客户端登录用户线的认证方式为 AAA 认证。

```
[AC] line vty 0 63
[AC-line-vty0-63] authentication-mode scheme
[AC-line-vty0-63] quit
```

创建设备管理类本地用户 client001，并设置密码为明文 aabbcc，服务类型为 SSH，用户角色为 network-admin。

```
[AC] local-user client001 class manage
[AC-luser-manage-client001] password simple aabbcc
[AC-luser-manage-client001] service-type ssh
[AC-luser-manage-client001] authorization-attribute user-role network-admin
[AC-luser-manage-client001] quit
```

配置 SSH 用户 client001 的服务类型为 NETCONF，认证方式为 password 认证。（此步骤可以不配置）

```
[AC] ssh user client001 service-type netconf authentication-type password
```

10.3 验证配置

用户通过支持 NETCONF over SSH 连接的客户端软件与 AC 建立 NETCONF over SSH 连接之后，可直接进入 AC 的 NETCONF 配置模式。

打开支持 NETCONF over SSH 登录方式的客户端软件，本文以 NetConf Browser 2015（Version3.1）工具为例。

在菜单栏中选择“File> Connect…”。

- “NETCONF version”选择“Auto select”。
- “Host”文本框处输入设备 IP“192.168.100.49”。

- “Port”文本框处输入“830”。
- “Username”文本框处输入“client001”。
- 单击“Connect”按钮完成设置。

图18 通过 NetConf Browser 连接设备

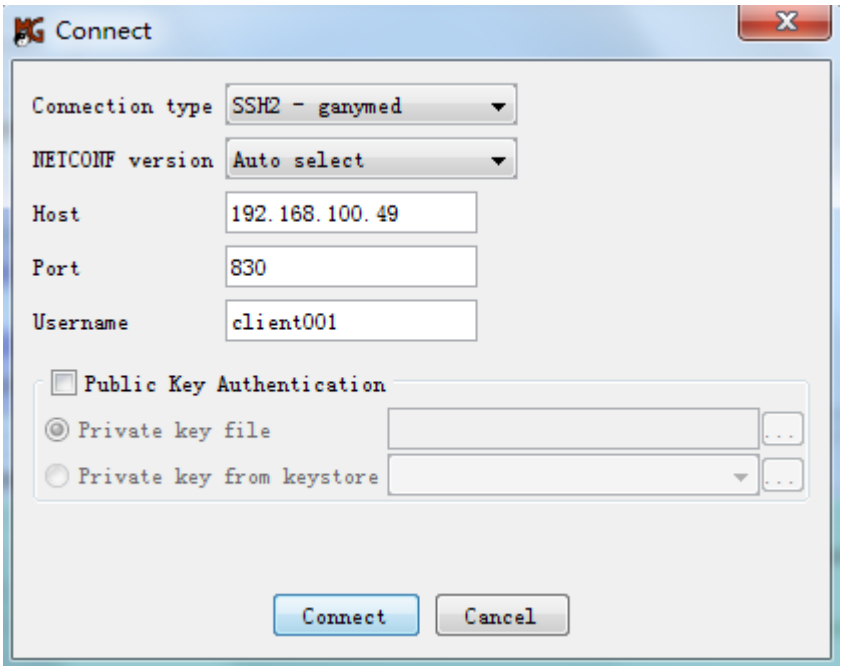


图19 输入密码：aabbcc。

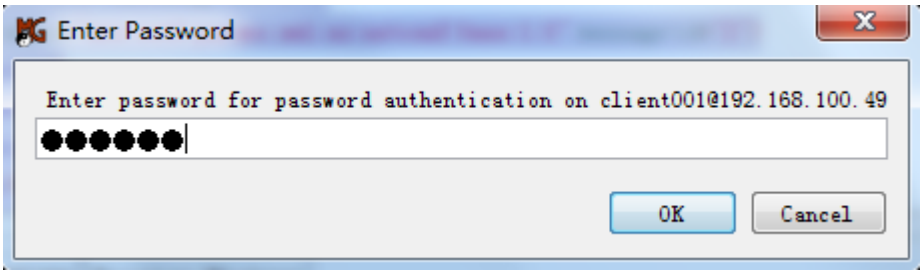
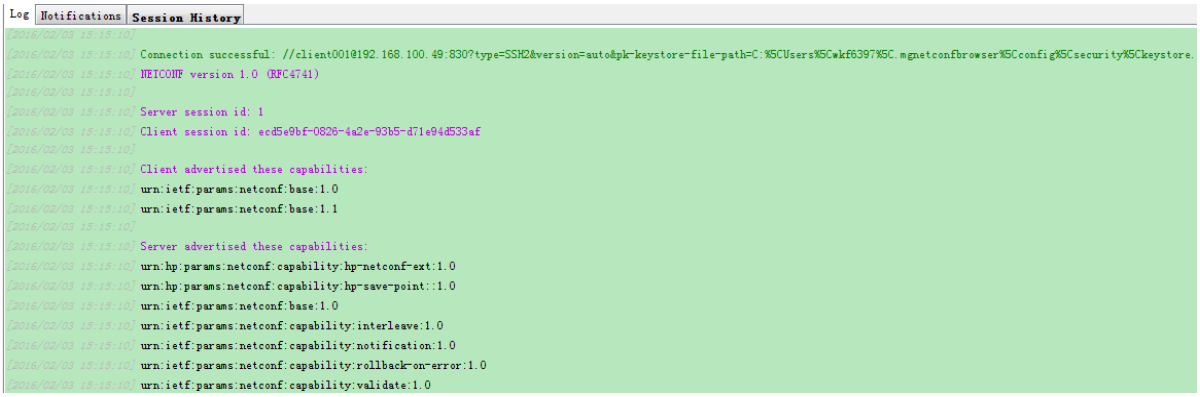


图20 登录成功



与 AC 建立 NETCONF over SSH 连接之后，直接进入 AC 的 NETCONF 配置模式。用户登录时获得 network-admin 权限，例如：

在 NetConf Browser 的“Command XML”区域输入以下信息，并点击 Send：

```
<get-sessions/>
```

在“Output XML”区域显示 NETCONF 用户的会话信息。

```
<?xml version="1.0" encoding="utf-8"?>
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="2">
  <get-sessions>
    <Session>
      <SessionID>1</SessionID>
      <Line>vty1</Line>
      <UserName>client001</UserName>
      <Since>2011-01-01T08:36:27</Since>
      <LockHeld>false</LockHeld>
    </Session>
  </get-sessions>
</rpc-reply>
```

11 相关资料

- 《H3C 无线控制器产品 配置指导》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“安全命令参考。
- 《H3C 无线控制器产品 配置指导》中的“WLAN 接入配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 接入命令参考”。