H3C SSH Configuration Examples

Software version: Release 7595

Document version: 6W100-20201031

Contents

Introduction

This document provides SSH configuration examples.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of SSH.

General restrictions and guidelines

The devices in the configuration examples operate in non-FIPS mode.

When you configure SSH on a device that operates in FIPS mode, follow these restrictions and guidelines:

- The modulus length of the key pair must be 2048 bits.
- When the device acts as an SSH server, only ECDSA and RSA key pairs are supported. Do not generate a DSA key pair on the SSH server.

Example: Configuring the device as an Stelnet server using password authentication

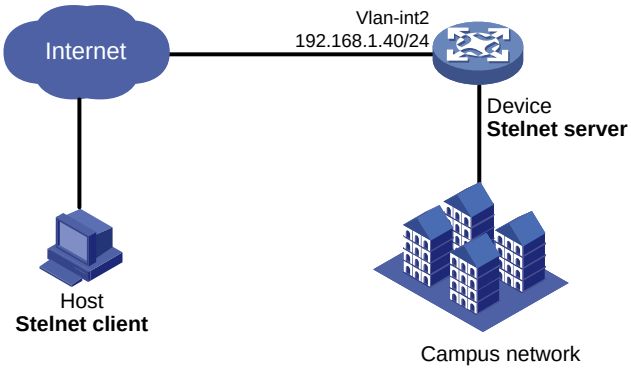
Network configuration

As shown in Figure 1:

- The device uses local password authentication.
- The login username and password are **client001** and **aabbcc**, respectively.

Establish an Stelnet connection between the host and the device, so you can log in to the device to manage the campus network.

Figure 1 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- To ensure correct SSH version negotiation and algorithm negotiation, and to ensure that the server can pass the client's authentication, generate DSA, ECDSA, and RSA key pairs on the server.
- To perform local authentication, create a local user and configure a password for the local user on the Stelnet server.
- To enable an SSH user to use all commands after login, set the user role of the local user to **network-admin**. By default, the user role of a local user is network-operator.
- The authentication mode for Stelnet user lines must be AAA (**scheme**).

Procedures

Generate RSA key pairs.

```
<Device> system-view
[Device] 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.
```

Generate a DSA key pair.

```
[Device] 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.
```

Generate an ECDSA key pair.

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

Enable the SSH server function.

```
[Device] ssh server enable
```

Create VLAN 2, and assign Ten-GigabitEthernet 1/0/2 to VLAN 2.

```
[Device] vlan 2
[Device-vlan2] port ten-gigabitethernet 1/0/2
[Device-vlan2] quit
```

Assign an IP address to VLAN-interface 2. The Stelnet client uses the IP address as the destination address of the Stelnet connection.

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

Set the authentication mode to AAA (**scheme**) for the user lines.

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

Create a local user **client001**.

```
[Device] local-user client001 class manage
New local user added.
```

Set the password to **aabbcc** in plain text for the local user **client001**.

```
[Device-luser-manage-client001] password simple aabbcc
```

Authorize the local user **client001** to use the **SSH** service.

```
[Device-luser-manage-client001] service-type ssh
```

Assign the user role **network-admin** to the local user **client001**.

```
[Device-luser-manage-client001] authorization-attribute user-role network-admin
[Device-luser-manage-client001] quit
```

Verifying the configuration

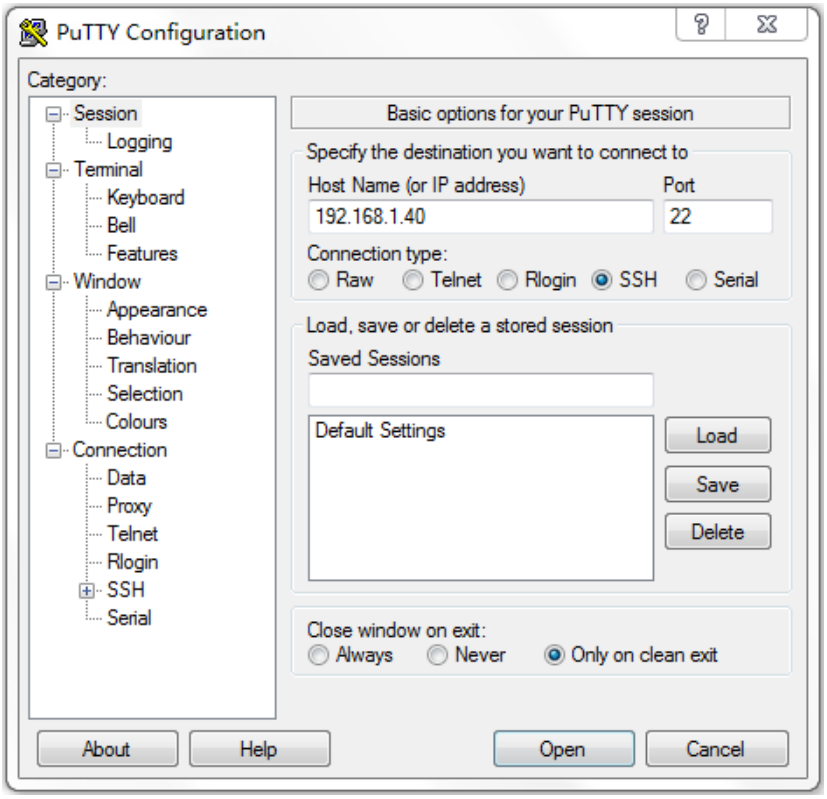
There are different types of Stelnet client software, including PuTTY and OpenSSH. This example uses an Stelnet client that runs Putty version 0.60.

To verify that you can log in to the Stelnet server from the Stelnet client:

1. Launch PuTTY.exe.
2. From the navigation tree, click **Session**.

   The interface shown in Figure 2 appears.
3. In the **Specify the destination you want to connect to** area, configure the following parameters:
   a. Enter **192.168.1.40** in the **Host Name (or IP address)** field.
   b. Enter **22** in the **Port** field.
   c. Select **SSH** for **Connection type**.

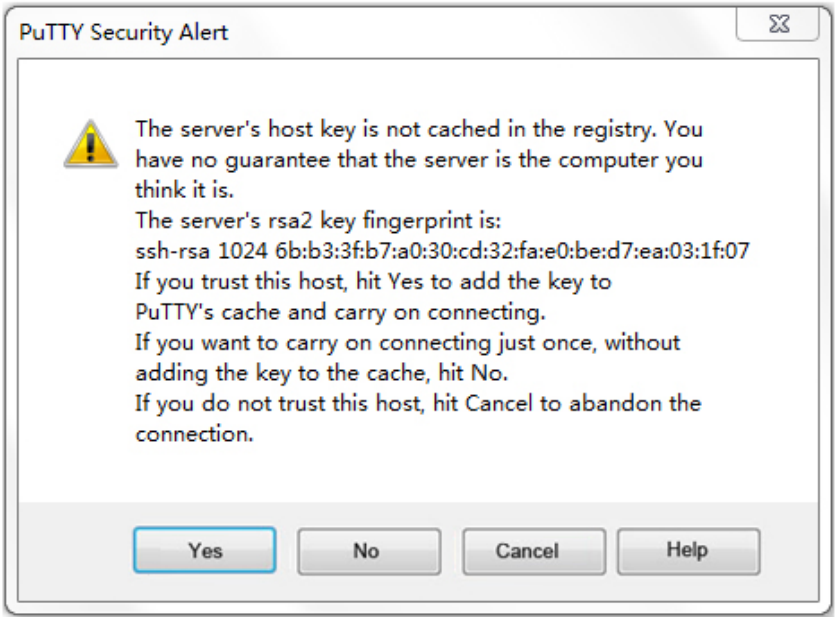
Figure 2 Specifying basic connection parameters



4. Click **Open**.

   The dialog box shown in Figure 3 appears.

   Figure 3 PuTTY Security Alert dialog box



5. Click **Yes**.
6. Enter the username **client001** and the password **aabbcc** to log in to the Stelnet server.

```
login as: client001
```

```
client001@192.168.1.40's password:

******************************************************************************
* Copyright (c) 2004-2010 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

<Device>
```

Configuration files

```
#
vlan 2
#
interface Vlan-interface2
 ip address 192.168.1.40 255.255.255.0
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
line vty 0 63
 authentication-mode scheme
#
ssh server enable
#
local-user client001 class manage
 password hash $h$6$CqMnWdX6LIW/hz2Z$4+0Pumk+A98VlGVgqN3n/mEi7hJka9fEZpRZIpSNi9b
cBEXhpvIqaYTvIVBf7ZUNGnovFsqW7nYxjoToRDvYBg==
 service-type ssh
 authorization-attribute user-role network-admin
 authorization-attribute user-role network-operator
#
```

Example: Configuring the device as an Stelnet server using publickey authentication

Network configuration

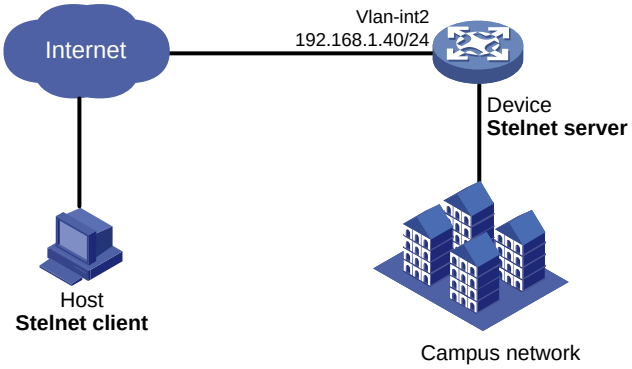
As shown in Figure 4:

- The device uses publickey authentication and RSA public key algorithm.
- The login username is **client001**.

Establish an Stelnet connection between the host and the device, so you can log in to the device to manage the campus network.

Import the client's host public key to the server to ensure correct format and content of the public key.

Figure 4 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- Because the client's host public key is required in the server configuration, you must generate RSA key pairs on the client before configuring the server.
- For successful publickey authentication, perform the following tasks:
  a. Configure the client's RSA host public key on the server.
  b. Specify the paired RSA host private key for the SSH user on the client.
- The authentication mode for Stelnet user lines must be AAA (**scheme**).
- To assign the correct working directory and user role to the SSH user, you must create a local user on the Stelnet server. The local user must have the same username as the SSH user. To enable an SSH user to use all commands after login, set the user role of the local user to **network-admin**. By default, the user role of a local user is network-operator.

Restrictions and guidelines

When you configure the device as an Stelnet server using publickey authentication, follow these restrictions and guidelines:

- In FIPS mode, the Stelnet server does not support publickey authentication.
- To support Stelnet clients that use different types of key pairs, generate DSA, ECDSA, and RSA key pairs on the Stelnet server.

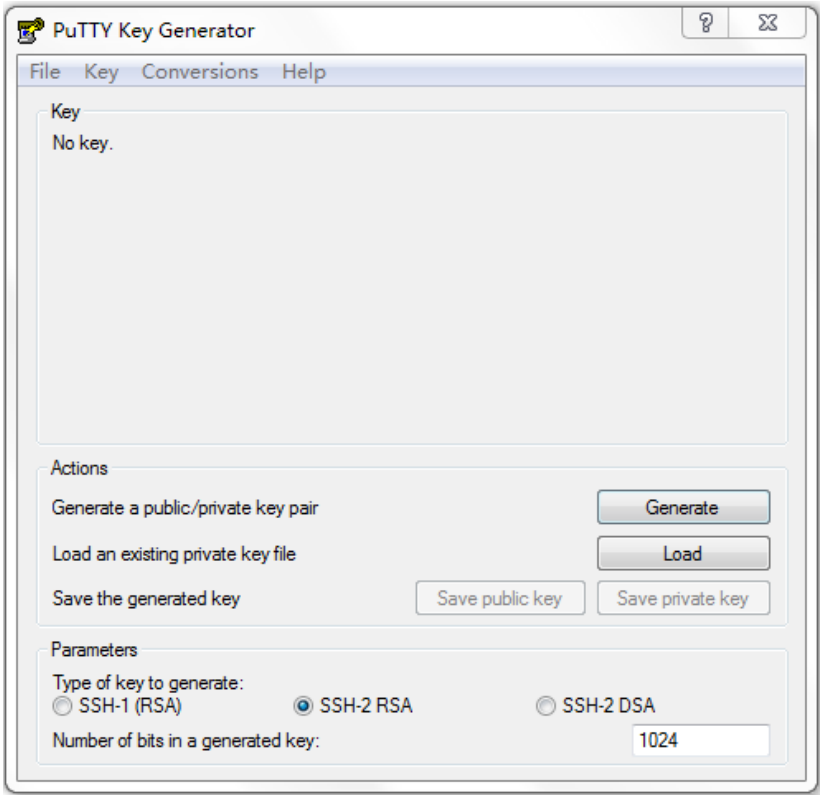
Procedures

Configuring the host as an Stelnet client

There are different types of Stelnet client software, including PuTTY and OpenSSH. This example uses an Stelnet client that runs Putty version 0.60.

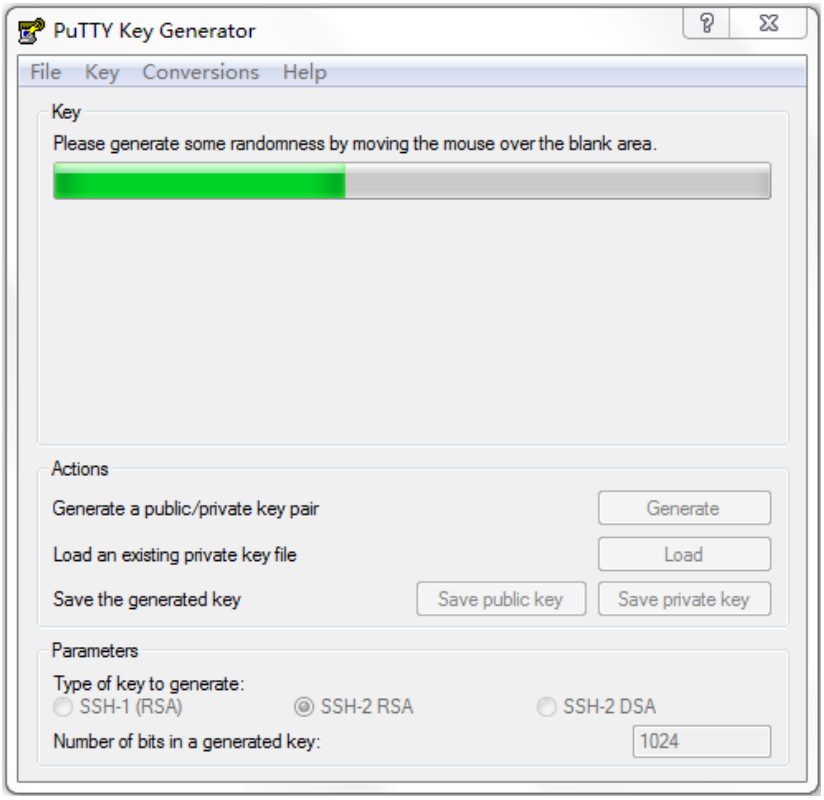
1. Run PuTTYGen.exe, select **SSH-2 RSA**, and click **Generate**.

Figure 5 Generating a key pair on the client



2. Continuously move the mouse and do not place the mouse over the green process bar shown in Figure 6. Otherwise, the process bar stops moving and the key pair generating process stops.

Figure 6 Generating process

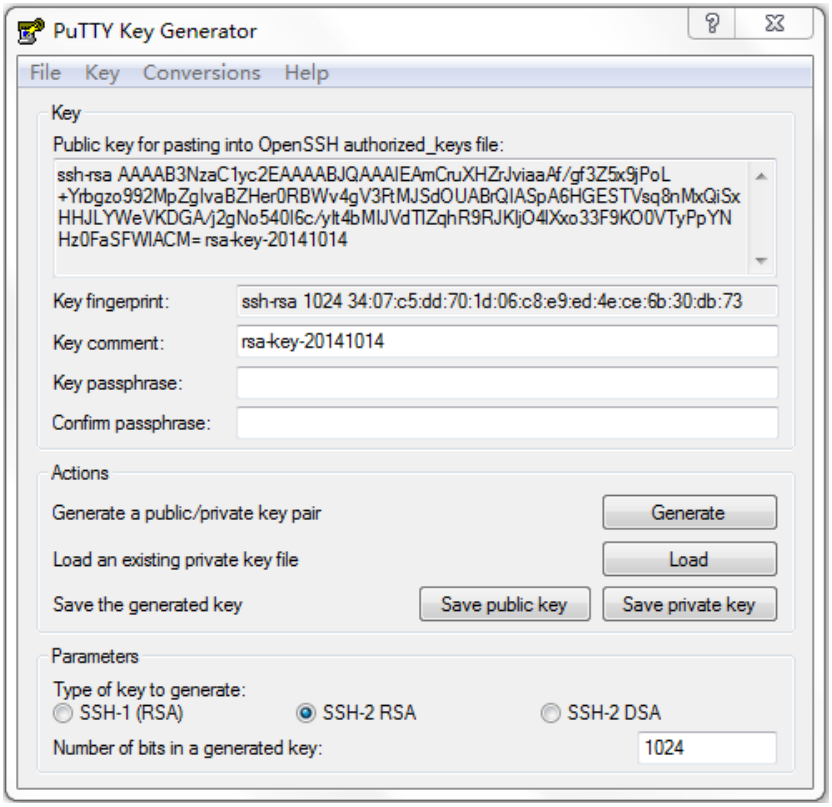


3. After the key pair is generated, click **Save public key**.

   A file saving window appears.

4. Select the saving directory (disk D in this example), enter a file name (**key.pub** in this example), and click **Save**.

Figure 7 Saving a key pair on the client



5. On the page shown in Figure 7, click **Save private key**.

   A confirmation dialog box appears.

6. Click **Yes**.

   A file saving window appears.

7. Select the saving directory (disk D in this example), enter a file name (**private.ppk** in this example), and click **Save**.

Configuring the device as the FTP server

Create VLAN 2, and assign Ten-GigabitEthernet 1/0/2 to VLAN 2.

```
<Device> system-view
[Device] vlan 2
[Device-vlan2] port ten-gigabitethernet 1/0/2
[Device-vlan2] quit
```

Assign an IP address to VLAN-interface 2.

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

Create a local user **ftp**.

```
[Device] local-user ftp class manage
New local user added.
```

Set the password to **ftp** in plain text for the local user **ftp**.

```
[Device-luser-manage-ftp] password simple ftp
```

Assign the user role **network-admin** to the local user **ftp**.

```
[Device-luser-manage-ftp] authorization-attribute user-role network-admin
```

Assign the working directory **flash:/** to the local user **ftp**.

```
[Device-luser-manage-ftp] authorization-attribute work-directory flash:/
```

Authorize the local user **ftp** to use the **FTP** service.

```
[Device-luser-manage-ftp] service-type ftp
[Device-luser-manage-ftp] quit
```

Enable the FTP server function.

```
[Device] ftp server enable
[Device] quit
```

Uploading the public key file from the FTP client

Log in to the FTP server from the host and upload the public key file **key.pub** to the server.

```
<Host>ftp 192.168.1.40
Press CTRL+C to abort.
Connected to 192.168.1.40 (192.168.1.40).
220 FTP service ready.
User (192.168.1.56:(none)): ftp
331 Password required for ftp.
Password:
230 User logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> put flash:/key.pub
227 Entering Passive Mode (192,168,1,40,41,116)
150 Accepted data connection
226 File successfully transferred
301 bytes sent in 0.000 seconds (1.05 Mbytes/s)
ftp> quit
221-Goodbye. You uploaded 1 and downloaded 0 kbytes.
221 Logout.
```

Configuring the device as the Stelnet server

Generate RSA key pairs.

```
[Device] 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.
```

Generate a DSA key pair.

```
[Device] 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.
```

Generate an ECDSA key pair.

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

Enable the SSH server function.

```
[Device] ssh server enable
```

Set the authentication mode to AAA (**scheme**) for the user lines.

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

Import the client's public key from the file **key.pub**, and name the public key **devicekey**.

```
[Device] public-key peer devicekey import sshkey key.pub
```

Create an SSH user **client001**. Specify the authentication type as **publickey** for the user, and assign the public key **devicekey** to the user.

```
[Device] ssh user client001 service-type stelnet authentication-type publickey assign
publickey devicekey
```

Create a local user **client001**.

```
[Device] local-user client001 class manage
New local user added.
```

Authorize the local user **client001** to use the **SSH** service.

```
[Device-luser-manage-client001] service-type ssh
```

Assign the user role **network-admin** to the local user **client001**.

```
[Device-luser-manage-client001] authorization-attribute user-role network-admin
[Device-luser-manage-client001] quit
```

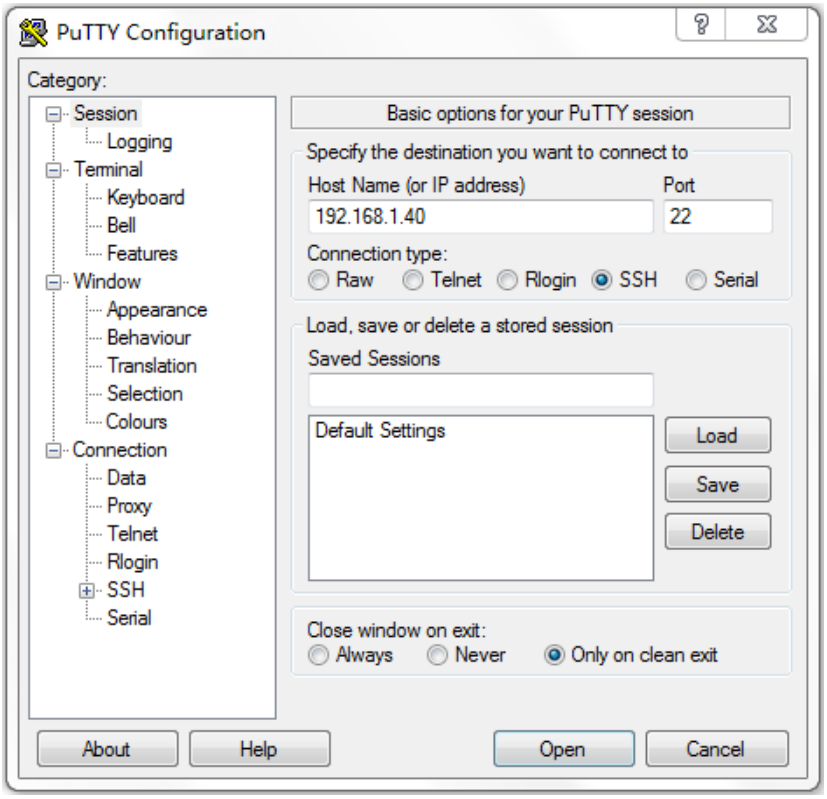
Verifying the configuration

To verify that you can log in to the Stelnet server from the Stelnet client:

1. Launch PuTTY.exe.
2. From the navigation tree, click **Session**.

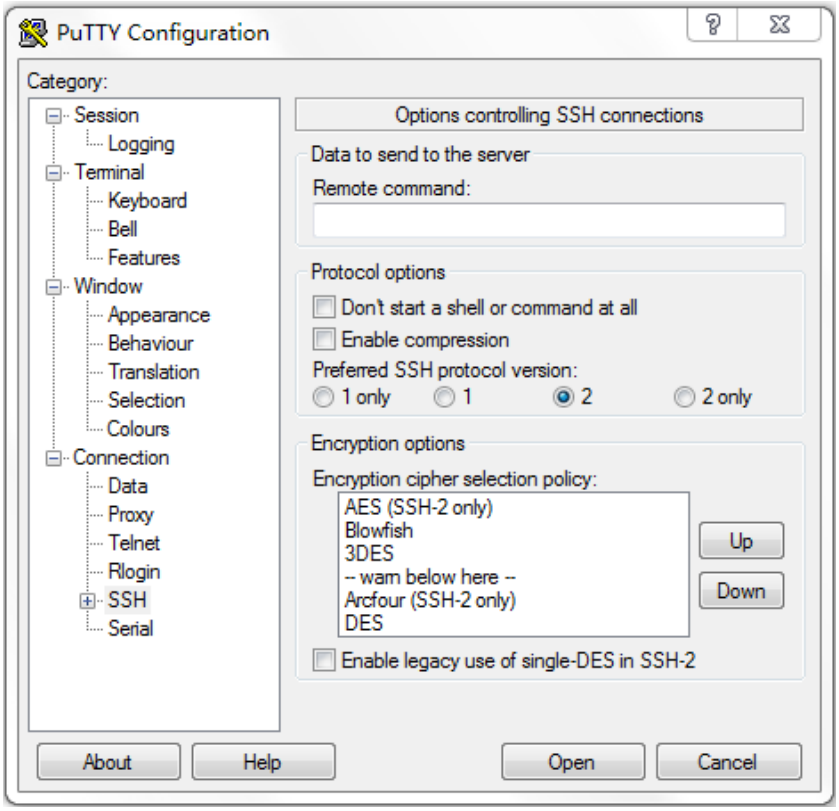
   The interface shown in Figure 8 appears.
3. In the **Specify the destination you want to connect to** area, configure the following parameters:
   a. Enter **192.168.1.40** in the **Host Name (or IP address)** field.
   b. Enter **22** in the **Port** field.
   c. Select **SSH** for **Connection type**.

Figure 8 Specifying basic connection parameters



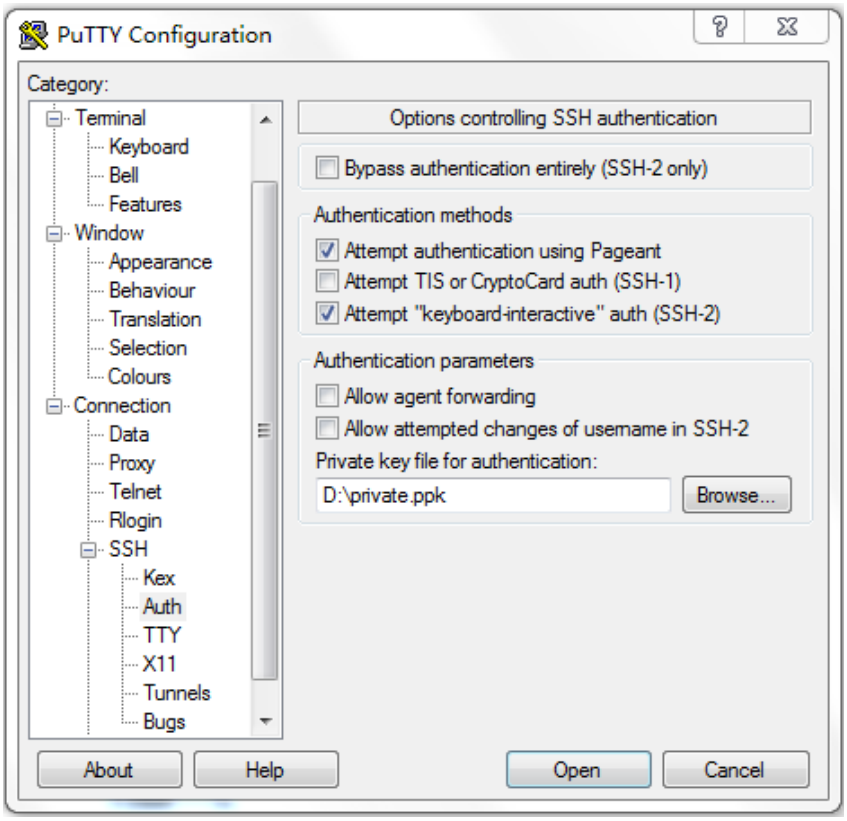
4. From the navigation tree, select **Connection** > **SSH**.
   The window shown in Figure 9 appears.
5. In the **Protocol options** area, specify the preferred SSH version as 2.

Figure 9 Specifying the SSH version



6. From the navigation tree, select **Connection** > **SSH** > **Auth**.
   The window shown in Figure 10 appears.
7. Click **Browse…**.
   A file selection window appears.
8. Select the private key file **private.ppk**, and click **OK**.

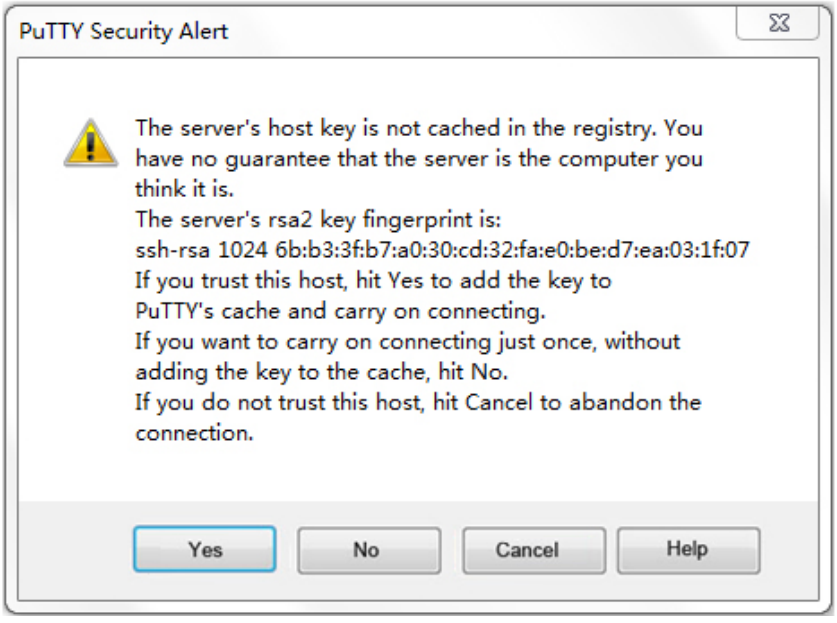
Figure 10 Specifying the private key file



9. Click **Open**.

   The dialog box shown in Figure 11 appears.

Figure 11 PuTTY Security Alert dialog box



10. Click **Yes**.
11. Enter the username **client001** to log in to the Stelnet server.

```
login as: client001
```

```
Authenticating with public key ”rsa-key-20200226”

******************************************************************************
* Copyright (c) 2004-2010 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

<Device>
```

Configuration files

```
#
vlan 2
#
interface Vlan-interface2
 ip address 192.168.1.40 255.255.255.0
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
line vty 0 63
 authentication-mode scheme
#
ssh server enable
ssh user client001 service-type stelnet authentication-type publickey assign publickey
devicekey
#
local-user client001 class manage
service-type ssh
 authorization-attribute user-role network-operator
 authorization-attribute user-role network-admin
#
public-key peer Devicekey
public-key-code begin
30819D300D06092A864886F70D010101050003818B0030818702818100A2DBC1FD76A837BEF5D32259844
2D6753B2E8F7ADD6D6209C80843B206B309078AFE2416CB4FAD496A6627243EAD766D57AEA70B901B4B45
66D9A651B133BAE34E9B9F04E542D64D0E9814D7E3CBCDBCAF28FF21EE4EADAE6DF52001944A40414DFF2
80FF043B14838288BE7F9438DC71ABBC2C28BF78F34ADF3D1C912579A19020125
public-key-code end
peer-public-key end
#
local-user ftp
password cipher $c$3$sg9WgqO1w8vnAv2FKGTOYgFJm3nn2w==
authorization-attribute work-directory flash:/
authorization-attribute user-role network-operator
service-type ftp
#
```

```
ftp server enable
#
```

Example: Configuring the device as an Stelnet client for password authentication

Network configuration

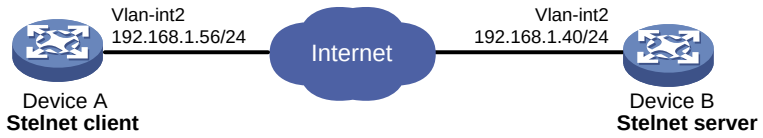
As shown in Figure 12:

- Device B uses local password authentication.
- The login username and password are **client001** and **aabbcc**, respectively.

Establish an Stelnet connection between Device A and Device B, so you can log in to Device B to use all commands and perform secure data exchange.

To ensure communication security, configure Device A to use the host public key of Device B to authenticate Device B.

Figure 12 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- To ensure correct SSH version negotiation and algorithm negotiation, and to ensure that the server can pass the client's authentication, generate DSA, ECDSA, and RSA key pairs on the server.
- The authentication mode for Stelnet user lines must be AAA (**scheme**).
- To perform local authentication, create a local user and configure a password for the local user on the Stelnet server.
- To enable an SSH user to use all commands after login, set the user role of the local user to **network-admin**. By default, the user role of a local user is network-operator.
- Because the Stelnet client uses the host public key of the server to authenticate the server, you must configure the host public key of the server on the client.

Procedures

Configuring the Stelnet server

Generate RSA key pairs.

```
<DeviceB> system-view
[DeviceB] 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.
```

Generate a DSA key pair.

```
[DeviceB] 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.
```

Generate an ECDSA key pair.

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

Enable the SSH server function.

```
[DeviceB] ssh server enable
```

Create VLAN 2, and assign Ten-GigabitEthernet 1/0/2 to VLAN 2.

```
[DeviceB] vlan 2
[DeviceB-vlan2] port ten-gigabitethernet 1/0/2
[DeviceB-vlan2] quit
```

Assign an IP address to VLAN-interface 2. The Stelnet client uses this address as the destination address of the Stelnet connection.

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

Set the authentication mode to AAA (**scheme**) for the user lines.

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

Create a local user **client001**.

```
[DeviceB] local-user client001 class manage
New local user added.
```

Set the password to **aabbcc** in plain text for the local user **client001**.

```
[DeviceB-luser-manage-client001] password simple aabbcc
```

Authorize the local user **client001** to use the **SSH** service.

```
[DeviceB-luser-manage-client001] service-type ssh
```

Assign the user role **network-admin** to the local user **client001**.

```
[DeviceB-luser-manage-client001] authorization-attribute user-role network-admin
[DeviceB-luser-manage-client001] quit
```

Display the DSA key pair of the server.

```
[DeviceB] display public-key local dsa public
```

```
=====================================================
Key name: dsakey (default)
Key type: DSA
Time when key pair created: 11:02:10 2020/02/07
Key code:

   308201B73082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD
   96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
   DBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941D
   DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
   7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
   4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
   35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
   91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
   585DA7F42519718CC9B09EEF03818400028180077F06B3E343CAE9988F4BE3F76FACBAB565
   AB73D4BA295C52BA92428B1F2DA1E6DD652413DD3AFE0C5A4FCF365100CBE34CECA55A2C30
   A2A9FF7E899628557E39CE8FC615F53193A7E200B4B1CB21E3F1091D595716D229DDED6872
   061F9B4B08301ADC81F7EC1501FFB863C0009536596CCB508596C3325892DC6D8C5C35B5
```

Configuring the Stelnet client

Create VLAN 2, and assign Ten-GigabitEthernet 1/0/2 to VLAN 2.

```
<DeviceA> system-view
[DeviceA] vlan 2
[DeviceA-vlan2] port ten-gigabitethernet 1/0/2
[DeviceA-vlan2] quit
```

Assign an IP address to VLAN-interface 2. The client uses this IP address to connect to the server.

```
[DeviceA] interface vlan-interface 2
[DeviceA-Vlan-interface2] ip address 192.168.1.56 255.255.255.0
[DeviceA-Vlan-interface2] quit
```

Specify the name of the server's host public key as **key1** and enter public key view.

```
[DeviceA] public-key peer key1
Enter public key view. Return to system view with "peer-public-key end" command.
```

Configure the host public key of the Stelnet server by entering the public key displayed by the **display public-key local dsa public** command. By default, the client authenticates the server by using the DSA host public key of the server.

```
[DeviceA-pkey-public-key-key1]308201B73082012C06072A8648CE3804013082011F02818100D7572
62C4584C44C211F18BD96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C26585
4889DC1EDBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941DDD7
7FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B368950387811C7DA330215
00C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E14EC474BAF2932E69D3B1F1851
7AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD35D02492B3959EC6499625BC4FA5082E22C5
B374E16DD00132CE71B020217091AC717B612391C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E8
10561C21621C73D6DAAC028F4B1585DA7F42519718CC9B09EEF03818400028180077F06B3E343CAE9988F
4BE3F76FACBAB565AB73D4BA295C52BA92428B1F2DA1E6DD652413DD3AFE0C5A4FCF365100CBE34CECA55
A2C30A2A9FF7E899628557E39CE8FC615F53193A7E200B4B1CB21E3F1091D595716D229DDED6872061F9B
4B08301ADC81F7EC1501FFB863C0009536596CCB508596C3325892DC6D8C5C35B5
```

Exit public key view.

```
[DeviceA-pkey-public-key-key1] peer-public-key end
[DeviceA] return
```

Verifying the configuration

Verify that you can log in to the Stelnet server from the Stelnet client. The host public key of the server is **key1**.

```
<DeviceA> ssh2 192.168.1.40 public-key key1
login as: client001
client001@192.168.1.40's password:

******************************************************************************
* Copyright (c) 2004-2010 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************


<DeviceB>
```

After you enter the username (**client001**) and the password (**aabbcc**), you can log in to the Stelnet server successfully.

Configuration files

- Device A:

```
#
vlan 2
#
interface Vlan-interface2
ip address 192.168.1.56 255.255.255.0
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
public-key peer key1
public-key-code begin
308201B73082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD
   96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
   DBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941D
   DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
   7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
   4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
   35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
   91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
   585DA7F42519718CC9B09EEF03818400028180077F06B3E343CAE9988F4BE3F76FACBAB565
   AB73D4BA295C52BA92428B1F2DA1E6DD652413DD3AFE0C5A4FCF365100CBE34CECA55A2C30
   A2A9FF7E899628557E39CE8FC615F53193A7E200B4B1CB21E3F1091D595716D229DDED6872
   061F9B4B08301ADC81F7EC1501FFB863C0009536596CCB508596C3325892DC6D8C5C35B5
```

```
public-key-code end
peer-public-key end
#
```

- Device B:

```
#
vlan 2
#
interface Vlan-interface2
 ip address 192.168.1.40 255.255.255.0
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
line vty 0 63
 authentication-mode scheme
#
ssh server enable
#
local-user client001
 password cipher $c$3$o71Exx1XIKs9gJoxqSodHGl1uT9rlZEd4w==
authorization-attribute user-role network-operator
 authorization-attribute user-role network-admin
 service-type ssh
#
```

Example: Configuring SFTP with password-publickey authentication

Network configuration

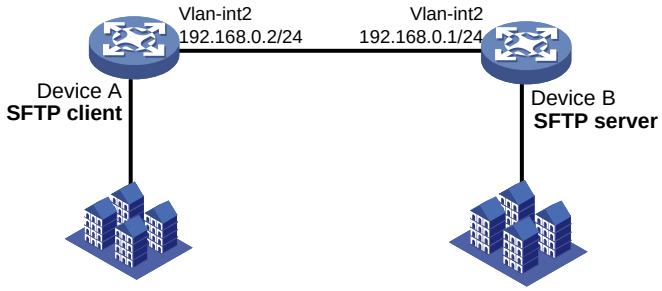
As shown in Figure 13:

- Device B uses password-publickey authentication and RSA public key algorithm.
- The login username and password are **client001** and **aabbcc**, respectively.

Establish an SFTP connection between Device A and Device B, so you can log in to Device B to perform file and directory operations.

Import the client's host public key to the server to ensure correct format and content of the public key.

Figure 13 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- Because the client's host public key is required in the server configuration, you must generate RSA key pairs on the client before configuring the SFTP server.
- For successful publickey authentication, perform the following tasks:
  a. Configure the client's RSA host public key on the server.
  b. Specify the paired RSA host private key for the SSH user on the client.

     To specify the RSA host private key on the client, use the **identity-key rsa** keyword in the **sftp** command.
- To perform local authentication, create a local user and configure a password for the local user on the SFTP server.
- To enable an SSH user to use all commands after login, set the user role of the local user to **network-admin**. By default, the user role of a local user is network-operator.
- To assign the correct working directory and user role to the SSH user, configure the local user to have the same username as the SSH user.

Restrictions and guidelines

When you configure SFTP with password-publickey authentication, follow these restrictions and guidelines:

- In FIPS mode, the SFTP server does not support publickey authentication.
- To support SFTP clients that use different types of key pairs, generate DSA, ECDSA, and RSA key pairs on the SFTP server.

Procedures

Configuring Device A as the SFTP client

Create VLAN 2, and assign Ten-GigabitEthernet 1/0/2 to VLAN 2.

```
<DeviceA> system-view
[DeviceA] vlan 2
[DeviceA-vlan2] port ten-gigabitethernet 1/0/2
[DeviceA-vlan2] quit
```

Assign an IP address to VLAN-interface 2. The client uses this address to connect to the server.

```
[DeviceA] interface vlan-interface 2
```

```
[DeviceA-Vlan-interface2] ip address 192.168.0.2 255.255.255.0
[DeviceA-Vlan-interface2] quit
```

Generate RSA key pairs.

```
[DeviceA] 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.
```

Export the host public key to the file **key.pub**.

```
[DeviceA] public-key local export rsa ssh2 key.pub
[DeviceA] quit
```

Configuring Device B as the FTP server

Create VLAN 2, and assign Ten-GigabitEthernet 1/0/2 to VLAN 2.

```
<DeviceB> system-view
[DeviceB] vlan 2
[DeviceB-vlan2] port ten-gigabitethernet 1/0/2
[DeviceB-vlan2] quit
```

Assign an IP address to VLAN-interface 2.

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

Create a local user **ftp**.

```
[DeviceB] local-user ftp class manage
New local user added.
```

Set the password to **ftp** in plain text for the local user **ftp**.

```
[DeviceB-luser-manage-ftp] password simple ftp
```

Assign the user role **network-admin** to the local user **ftp**.

```
[DeviceB-luser-manage-ftp] authorization-attribute user-role network-admin
```

Assign the working directory **flash:/** to the local user **ftp**.

```
[DeviceB-luser-manage-ftp] authorization-attribute work-directory flash:/
```

Authorize the local user **ftp** to use the **FTP** service.

```
[DeviceB-luser-manage-ftp] service-type ftp
[DeviceB-luser-manage-ftp] quit
```

Enable the FTP server function.

```
[DeviceB] ftp server enable
[DeviceB] quit
```

Uploading the public key file from the FTP client

Log in to the FTP server from Device A and upload the public key file **key.pub** to the server.

```
<DeviceA>ftp 192.168.0.1
```

```
Press CTRL+C to abort.
Connected to 192.168.0.1 (192.168.0.1).
220 FTP service ready.
User (192.168.0.2:(none)): ftp
331 Password required for ftp.
Password:
230 User logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> put flash:/key.pub
227 Entering Passive Mode (192,168,0,1,41,116)
150 Accepted data connection
226 File successfully transferred
301 bytes sent in 0.000 seconds (1.05 Mbytes/s)
ftp> quit
221-Goodbye. You uploaded 1 and downloaded 0 kbytes.
221 Logout.
```

Configuring Device B as the SFTP server

Generate RSA key pairs.

```
<DeviceB> system-view
[DeviceB] 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.
```

Generate a DSA key pair.

```
[DeviceB] 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.
```

Generate an ECDSA key pair.

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

Enable the SFTP server function.

```
[DeviceB] sftp server enable
```

Import the client's public key from the file **key.pub**, and name the public key **devicekey**.

```
[DeviceB] public-key peer devicekey import sshkey key.pub
```

Create an SSH user **client001**. Specify the authentication type as **password-publickey** for the user, and assign the public key **devicekey** to the user.

```
[DeviceB] ssh user client001 service-type sftp authentication-type password-publickey
assign publickey devicekey
```

Create a local user **client001**.

```
[DeviceB] local-user client001 class manage
New local user added.
```

Set the password to **aabbcc** in plain text for the local user **client001**.

```
[DeviceB-luser-manage-client001] password simple aabbcc
```

Authorize the local user **client001** to use the **SSH** service.

```
[DeviceB-luser-manage-client001] service-type ssh
```

Assign the user role **network-admin** and working directory **flash:/** to the local user **client001**.

```
[DeviceB-luser-manage-client001] authorization-attribute user-role network-admin
work-directory flash:/
[DeviceB-luser-manage-client001] quit
```

Verifying the configuration

1. Verify that you can log in to the SFTP server from the SFTP client.

   ```
   <DeviceA >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
   client001@192.168.0.1's password:
   ```

   After you enter the password, you are placed in SFTP client view.

   ```
   sftp>
   ```

2. Verify that you can perform file and directory operations after logging in to the SFTP server:

   # Display files under the current directory of the server, delete the file **z**, and verify the result.

   ```
   sftp> dir -l
   -rwxrwxrwx    1 1        1              1759 Aug 23 06:52 config.cfg
   -rw-rw----    1 1        1               301 Aug  7 16:52 key.pub
   -rwxrwxrwx    1 1        1                 0 Sep 01 06:22 new
   -rwxrwxrwx    1 1        1               225 Sep 01 06:55 pub
   -rwxrwxrwx    1 1        1               225 Aug 24 08:01 pubkey2
   -rwxrwxrwx    1 1        1                 0 Sep 01 08:00 z
   sftp> delete z
   Removing /z
   sftp> dir -l
   -rwxrwxrwx    1 1        1              1759 Aug 23 06:52 config.cfg
   -rw-rw----    1 1        1               301 Aug  7 16:52 key.pub
   -rwxrwxrwx    1 1        1                 0 Sep 01 06:22 new
   -rwxrwxrwx    1 1        1               225 Sep 01 06:55 pub
   -rwxrwxrwx    1 1        1               225 Aug 24 08:01 pubkey2
   ```

   # Add a directory **new1** and verify the result.

```
sftp> mkdir new1
sftp> dir -l
-rwxrwxrwx    1 1        1              1759 Aug 23 06:52 config.cfg
-rw-rw----    1 1        1               301 Aug  7 16:52 key.pub
-rwxrwxrwx    1 1        1                 0 Sep 01 06:22 new
drwxrwxrwx    1 1        1                 0 Sep 02 06:30 new1
-rwxrwxrwx    1 1        1               225 Sep 01 06:55 pub
-rwxrwxrwx    1 1        1               225 Aug 24 08:01 pubkey2
```

Rename directory **new1** to **new2** and verify the result.

```
sftp> rename new1 new2
sftp> dir -l
-rwxrwxrwx    1 1        1              1759 Aug 23 06:52 config.cfg
-rw-rw----    1 1        1               301 Aug  7 16:52 key.pub
-rwxrwxrwx    1 1        1                 0 Sep 01 06:22 new
drwxrwxrwx    1 1        1                 0 Sep 02 06:33 new2
-rwxrwxrwx    1 1        1               225 Sep 01 06:55 pub
-rwxrwxrwx    1 1        1               225 Aug 24 08:01 pubkey2
```

Download the file **pubkey2** from the server and change the name to **public**.

```
sftp> get pubkey2 public
Fetching /pubkey2 to public
/public                                       100%  301     0.3KB/s   00:00
```

Upload the local file **public** to the server, and verify the result.

```
sftp> put public
Uploading public to /public
public                                        100%  301     0.3KB/s   00:00
sftp> dir -l
-rwxrwxrwx    1 1        1              1759 Aug 23 06:52 config.cfg
-rw-rw----    1 1        1               301 Aug  7 16:52 key.pub
-rwxrwxrwx    1 1        1                 0 Sep 01 06:22 new
drwxrwxrwx    1 1        1                 0 Sep 02 06:33 new2
-rwxrwxrwx    1 1        1               225 Sep 01 06:55 pub
-rwxrwxrwx    1 1        1               225 Aug 24 08:01 pubkey2
-rwxrwxrwx    1 1        1               301 Jul 30 16:21 public
sftp>
```

Exit SFTP client view.

```
sftp> quit
<DeviceA>
```

Configuration files

- Device A:

```
#
vlan 2
#
interface Vlan-interface2
ip address 192.168.0.2 255.255.255.0
#
interface Ten-GigabitEthernet1/0/2
```

```
 port link-mode bridge
 port access vlan 2
#
```

- Device B:

```
#
vlan 2
#
interface Vlan-interface2
 ip address 192.168.0.1 255.255.255.0
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
sftp server enable
ssh user client001 service-type sftp authentication-type password-publickey assign
publickey devicekey
#
local-user client001 class manage
service-type ssh
password cipher $c$3$o71Exx1XIKs9gJoxqSodHGl1uT9rlZEd4w==
 authorization-attribute user-role network-operator
 authorization-attribute user-role network-admin
#
ftp server enable
#
local-user ftp class manage
 password simple ftp
 service-type ftp
 authorization-attribute user-role network-admin
 authorization-attribute user-role network-operator
#
public-key peer devicekey
 public-key-code begin
30819F300D06092A864886F70D010101050003818D00308189
1BD316C0DBB9009503E78F31947B651F9950E9A6E9E256E1E
 public-key-code end
 peer-public-key end
#
```

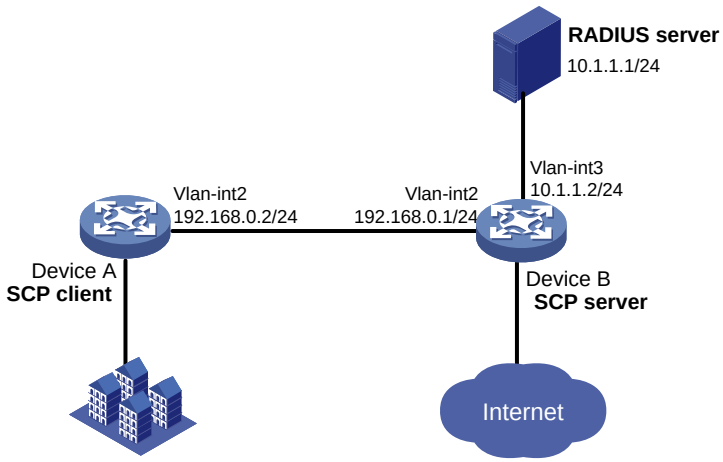
Example: Configuring SCP file transfer with remote password authentication

Network configuration

As shown in Figure 14, configure the devices and the RADIUS server to meet the following requirements:

- Establish an SCP connection between Device A and Device B, so you can log in to Device B to perform file transfer.
- Use the RADIUS server for SSH user authentication and authorization. The user name and password are **hello@bbb** and **aabbcc**, respectively.
- Include the domain name in the username sent to the RADIUS server.
- Assign the default user role **network-admin** to the SSH user, so the user can use all commands after login.

Figure 14 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- To ensure correct SSH version negotiation and algorithm negotiation, and to ensure that the server can pass the client's authentication, generate DSA, ECDSA, and RSA key pairs on the SSH server.
- To perform remote password authentication, configure the username and password on the RADIUS server. To enable an SSH user to use all commands after login, set the user role to **network-admin** for the user on the RADIUS server.
- To use the RADIUS server for authentication and authorization, perform the following tasks on Device B:
  a. Configure a RADIUS scheme to specify the authentication and authorization server.
  b. Create an ISP domain, and specify the ISP domain to use the RADIUS scheme for authentication, authorization, and accounting.
- To ensure communication security between the RADIUS client (Device B) and the RADIUS server, configure the same shared key on Device B and the RADIUS server.

Procedures

Configuring the RADIUS server

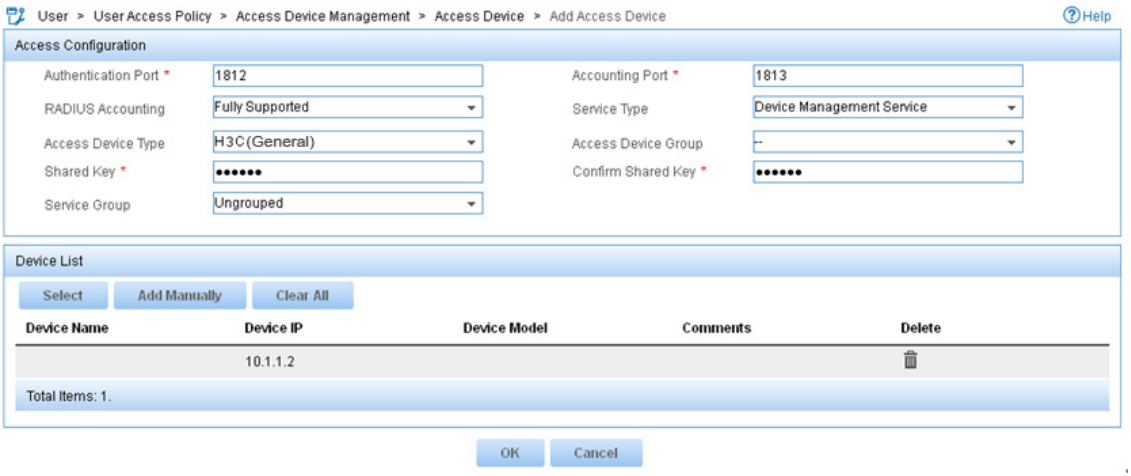
In this example, the RADIUS server runs on IMC PLAT 7.0 (E0102) and IMC UAM 7.0 (E0201).

Adding Device B to the IMC Platform as an access device

1. Log in to IMC.

2. Click the **User** tab.
3. From the navigation tree, select **User Access Policy**> **Access Device Management** > **Access Device**.
4. Click **Add**.
5. Configure an access device, as shown in Figure 15:
   a. Set the ports for authentication and accounting to **1812** and **1813**, respectively.
   b. Select the service type **Device Management Service**.
   c. Select the access device type **H3C(General)**.
   d. Set the shared key to **expert** for secure RADIUS communication.
   e. Select Device B from the device list or manually add Device B. (The IP address of Device B is 10.1.1.2).
   f. Use the default settings for other parameters.
6. Click **OK**.

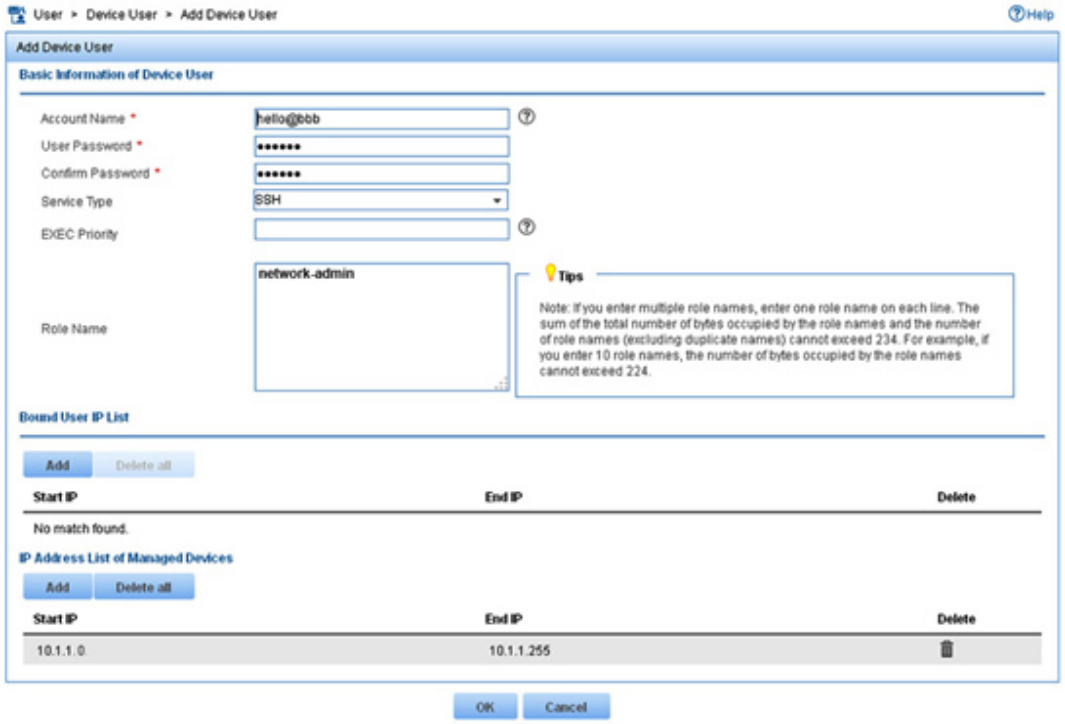
Figure 15 Adding Device B as an access device



Adding an account for device management

1. Click the **User** tab.
2. From the navigation tree, select **Access User** > **Device User**.
3. Click **Add**.
4. Configure a device management account, as shown in Figure 16:
   a. Enter the account name **hello@bbb** and the password **aabbcc**.
   b. Select the service type **SSH**.
   c. Enter the user role **network-admin** in the **Role Name** field.
   d. Specify **10.1.1.0** to **10.1.1.255** as the IP address range of the devices to be managed.
5. Click **OK**.

Figure 16 Adding a device management account



Configuring Device B

Generate RSA key pairs.

```
<DeviceB> system-view
[DeviceB] 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.
```

Generate a DSA key pair.

```
[DeviceB] 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.
```

Generate an ECDSA key pair.

```
[DeviceB] public-key local create ecdsa
Generating Keys...
.
```

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

Create VLAN 2, and assign Ten-GigabitEthernet 1/0/2 to VLAN 2.

```
[DeviceB] vlan 2
[DeviceB-vlan2] port ten-gigabitethernet 1/0/2
[DeviceB-vlan2] quit
```

Assign an IP address to VLAN-interface 2. The SCP client uses this address as the destination IP address of the SCP connection.

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

Create VLAN 3, and assign Ten-GigabitEthernet 1/0/1 to VLAN 3.

```
[DeviceB] vlan 3
[DeviceB-vlan3] port ten-gigabitethernet 1/0/1
[DeviceB-vlan3] quit
```

Assign an IP address to VLAN-interface 3. Device B uses this address to communicate with the RADIUS server.

```
[DeviceB] interface vlan-interface 3
[DeviceB-Vlan-interface3] ip address 10.1.1.2 255.255.255.0
[DeviceB-Vlan-interface3] quit
```

Enable the SSH server function.

```
[DeviceB] ssh server enable
```

Create a RADIUS scheme **rad**.

```
[DeviceB] radius scheme rad
```

Specify the primary authentication server 10.110.1.1 and UDP port 1812 for the RADIUS scheme **rad**.

```
[DeviceB-radius-rad] primary authentication 10.1.1.1 1812
```

Specify the primary authentication server 10.110.1.1 and UDP port 1813 for the RADIUS scheme **rad**.

```
[DeviceB-radius-rad] primary accounting 10.1.1.1 1813
```

Specify the shared key as **expert** for secure authentication and accounting communication.

```
[DeviceB-radius-rad] key authentication simple expert
[DeviceB-radius-rad] key accounting simple expert
```

Include domain names in the usernames sent to the RADIUS server.

```
[DeviceB-radius-rad] user-name-format with-domain
[DeviceB-radius-rad] quit
```

Create an ISP domain **bbb**.

```
[DeviceB] domain bbb
```

Configure ISP domain **bbb** to use RADIUS scheme **rad** for authentication, authorization, and accounting of all login users.

```
[DeviceB-isp-bbb] authentication login radius-scheme rad
[DeviceB-isp-bbb] authorization login radius-scheme rad
[DeviceB-isp-bbb] accounting login radius-scheme rad
[DeviceB-isp-bbb] quit
```

Configuring Device A

Create VLAN 2, and assign Ten-GigabitEthernet 1/0/2 to VLAN 2.

```
<DeviceA> system-view
[DeviceA] vlan 2
[DeviceA-vlan2] port ten-gigabitethernet 1/0/2
[DeviceA-vlan2] quit
```

Assign an IP address to VLAN-interface 2.

```
[DeviceA] interface vlan-interface 2
[DeviceA-Vlan-interface2] ip address 192.168.0.2 255.255.255.0
[DeviceA-Vlan-interface2] quit
[DeviceA] quit
```

Verifying the configuration

Verify that you can log in to the SCP server, download the file **remote.bin** from the server, and save it locally with the name **local.bin**.

```
<DeviceA> scp 192.168.0.1 get remote.bin local.bin
Username: hello@bbb
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
hello@bbb@192.168.0.1's password:
remote.bin                    100% 8275KB 318.3KB/s   00:26.
```

Configuration files

- Device A:

```
#
vlan 2
#
interface Vlan-interface2
ip address 192.168.0.2 255.255.255.0
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
```

- Device B:

```
#
vlan 2 to 3
#
interface Vlan-interface2
 ip address 192.168.0.1 255.255.255.0
#
interface Vlan-interface3
```

```
 ip address 10.1.1.2 255.255.255.0
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 3
#
ssh server enable
#
radius scheme rad
 primary authentication 10.1.1.1
 primary accounting 10.1.1.1
 key authentication cipher $c$3$63G7LzIQElGq4aFGTiYQafU+loQxS/cbLg==
 key accounting cipher $c$3$tUIVlyGISJ5X/yiTFWrmh8nyjBIF+1LFzQ==
#
domain bbb
 authentication login radius-scheme rad
 authorization login radius-scheme rad
 accounting login radius-scheme rad
#
```

Example: Configuring NETCONF over SSH with password authentication

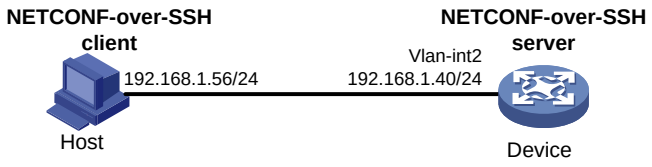
Network configuration

As shown in Figure 17:

- The device uses local password authentication.
- The client's username **client001** and password **aabbcc** are saved on the device.

Establish a NETCONF-over-SSH connection between the host and the device, so that you can perform NETCONF operations after logging in to the device.

Figure 17 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- To ensure correct SSH version negotiation and algorithm negotiation, and to ensure that the server can pass the client's authentication, generate DSA, ECDSA, and RSA key pairs on the SSH server.
- The authentication mode for SSH user lines must be AAA (**scheme**).
- To perform local authentication, create a local user and configure a password for the local user on the device. To enable an SSH user to perform NETCONF operations after login, set the user role of the local user to **network-admin**. By default, the user role of a local user is network-operator.

Procedures

Generate RSA key pairs.

```
<Device> system-view
[Device] 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.
```

Generate a DSA key pair.

```
[Device] 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.
```

Generate an ECDSA key pair.

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

#Create VLAN 2, and assign Ten-GigabitEthernet 1/0/2 to VLAN 2.

```
[Device] vlan 2
[Device-vlan2] port ten-gigabitethernet 1/0/2
[Device-vlan2] quit
```

Assign an IP address to VLAN-interface 2. The client uses this address as the destination address of the NETCONF-over-SSH connection.

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

Enable NETCONF over SSH.

```
[Device] netconf ssh server enable
```

Set the authentication mode to AAA (**scheme**) for the user lines.

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

Create a local device management user **client001**.

```
[Device] local-user client001 class manage
New local user added.
```

Set the password to **aabbcc** in plain text for the local user **client001**.

```
[Device-luser-manage-client001] password simple aabbcc
```

Authorize the local user **client001** to use the **SSH** service.

```
[Device-luser-manage-client001] service-type ssh
```

Assign the user role **network-admin** to the user.

```
[Device-luser-manage-client001] authorization-attribute user-role network-admin
[Device-luser-manage-client001] quit
```

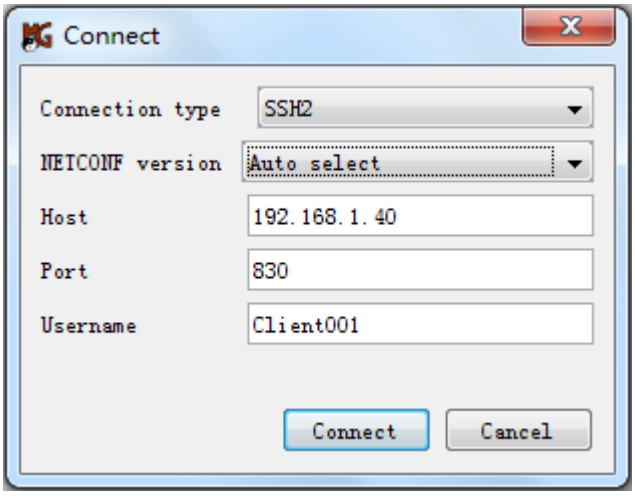
Verifying the configuration

This example uses NetConf Browser 2013 (version 3.1).

To verify that you can log in to the NETCONF-over-SSH server and perform NETCONF operations:

1. Launch NetConf Browser 2013 (version 3.1).
2. Select **File** > **Connect…** from the menu.
   a. Select **Auto select** from the **NETCONF version** list.
   b. Enter **192.168.1.40** in the **Host** field.
   c. Enter **830** in the **Port** field.
   d. Enter **Client001** in the **Username** field.
3. Click **Connect**.

Figure 18 Connecting to the device



4. Enter the password **aabbcc**, and click **OK**.
   The page shown in Figure 20 appears, and you enter the NETCONF configuration interface.

Figure 19 Entering the password

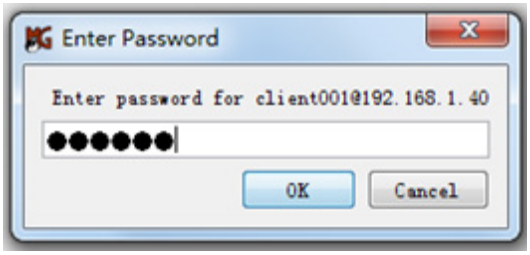
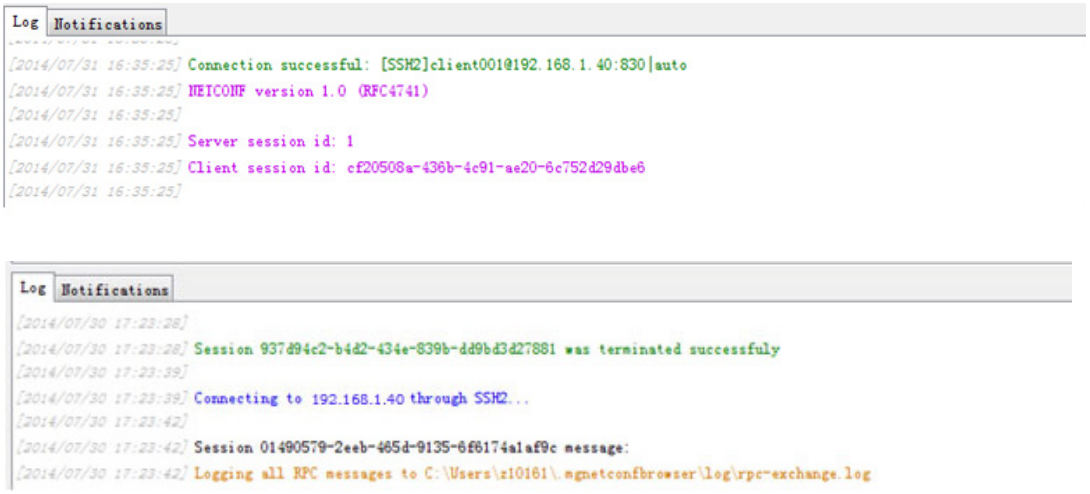


Figure 20 Logging in to the device



5. Enter **<get-sessions/>** in the **Command XML** area.

   The following message is displayed in the **Output XML** area.

```
<?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>2020-01-01T08:36:27</Since>
      <LockHeld>false</LockHeld>
    </Session>
  </get-sessions>
</rpc-reply>
```

Configuration files

```
#
vlan 2
#
interface Vlan-interface2
 ip address 192.168.1.40 255.255.255.0
#
```

```
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
line vty 0 63
 authentication-mode scheme
#
netconf ssh server enable
#
local-user client001 class manage
 password hash $h$6$CqMnWdX6LIW/hz2Z$4+0Pumk+A98VlGVgqN3n/mEi7hJka9fEZpRZIpSNi9b
cBEXhpvIqaYTvIVBf7ZUNGnovFsqW7nYxjoToRDvYBg==
 service-type ssh
 authorization-attribute user-role network-admin
 authorization-attribute user-role network-operator
#
```

Related documentation

- *H3C S7500X Switch Series Security Command Reference-R759X*
- *H3C S7500X Switch Series Security Configuration Guide-R759X*