**STelnet Login and Management**

Student Version



Huawei Technologies Co., Ltd.

|  |
| --- |
| **Copyright © Huawei Technologies Co., Ltd. 2020. All rights reserved.**  No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.  **Trademarks and Permissions**  HW_POS_RBG_Vertical-150ppi.png and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.  All other trademarks and trade names mentioned in this document are the property of their respective holders.  **Notice**  The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.  The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied. |

|  |  |
| --- | --- |
| Huawei Technologies Co., Ltd. | |
| Address: | Huawei Industrial Base  Bantian, Longgang  Shenzhen 518129  People's Republic of China |
| Website: | <https://e.huawei.com/> |

**Huawei Certification System**

Huawei Certification follows the "platform + ecosystem" development strategy, which is a new collaborative architecture of ICT infrastructure based on "Cloud-Pipe-Terminal". Huawei has set up a complete certification system consisting of three categories: ICT infrastructure certification, platform and service certification, and ICT vertical certification. It is the only certification system that covers all ICT technical fields in the industry. Huawei offers three levels of certification: Huawei Certified ICT Associate (HCIA), Huawei Certified ICT Professional (HCIP), and Huawei Certified ICT Expert (HCIE). Huawei Certification covers all ICT fields and adapts to the industry trend of ICT convergence. With its leading talent development system and certification standards, it is committed to fostering new ICT talent in the digital era, and building a sound ICT talent ecosystem.

Huawei Certified ICT Associate-Datacom (HCIA-Datacom) is designed for Huawei's frontline engineers and anyone who want to understand Huawei's datacom products and technologies. The HCIA-Datacom certification covers routing and switching principles, basic WLAN principles, network security basics, network management and O&M basics, SDN and programmability and automation basics.

The Huawei certification system introduces the industry, fosters innovation, and imparts cutting-edge datacom knowledge.



# STelnet Login and Management

## Background

During O&M, Telnet can implement remote login and management. However, during Telnet communication, all communication information, including the user name and password for remote login, is transmitted in plaintext, which is insecure. STelnet login can be used with SSH to prevent security risks caused by Telnet login and provide secure remote login on an insecure network. In this exercise, the administrator sets up the STelnet login environment through the console port and performs a login test.

## Objectives

Upon completion of this task, you will be able to:

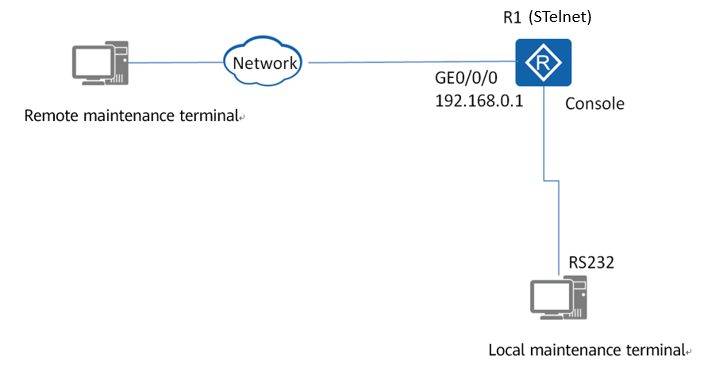
Understand the remote login process.

Configure STelnet login when the SSH user authentication mode is password authentication.

Configure STelnet login when the SSH user authentication mode is RSA authentication.

## Topology

Lab topology



Topology description:

1. In an exercise, the local and remote maintenance terminals can be the same PC.
2. For simplicity purposes, the device to be maintained and the remote maintenance terminal can be in the same network segment. In actual O&M, you can remotely log in to the device from the remote maintenance terminal through the Internet when the terminal can communicate with the device at Layer 3.

## Implementation

### Roadmap

1. Use the terminal emulation software to log in to the device through the console port of the device.
2. Configure device names and IPv4 addresses.
3. Configure the VTY user interface, including the user privilege level, authentication mode, and SSH protocol.
4. Create a user for STelnet login in the AAA view.
5. Enable the STelnet server, and create a local RSA key pair.
6. Set the SSH user authentication mode to password authentication and test the login.
7. Set the SSH user authentication mode to RSA authentication and test the login.

### Procedure

Use the terminal emulation software to log in to the device through the console port. For details, see "Console Login and Management".

Set the device name to **R1** and configure an IP address for GE0/0/0.

Configure VTY user interfaces.

#Set the maximum number of STelnet users to 15 (The value range varies according to product versions and models). By default, the maximum number of STelnet users is 5.

[R1]

#Access the VTY user interface view and set the authentication mode to AAA.

[R1]

#Set the user privilege level to level 3 (the default level is 0). VTY user interfaces support STelnet.

[R1]

Create two local users for STelnet login. Set the user names to **huawei01** and **huawei02**, password to **huawei123**, user privilege level to **level 3**, and service type to **ssh**.

[R1]

Enable the STelnet server and create a local RSA key pair.

#Enable the STelnet server.

[R1]

#Create a local RSA key pair.

[R1]

#Check the public key in the local key pair.

[R1]display rsa local-key-pair public

=====================================================

Time of Key pair created: 2020-05-05 11:16:46-08:00

Key name: Host

Key type: RSA encryption Key

=====================================================

Key code:

3047

0240

E11A43C6 8C4B0DF5 236B115C 41015514 024B1471

256EBDCE 862CEB50 052AB10D 010B1439 304E768C

2FB6844F EF2237FE C7BD0E84 AD350D0F 24BC8496

EE2F5EC9

0203

010001

=====================================================

Time of Key pair created: 2020-05-05 11:16:49-08:00

Key name: Server

Key type: RSA encryption Key

=====================================================

Key code:

3067

0260

B5FE13BD BAA84E09 BB355BA0 CA9FD405 D4927B10

CF01BDFD BE232946 C8FCE39F 146B779A C306FDB8

F2262214 4D70544E CAEE5424 D1C2CB61 69710F1A

4F50697E 6540D404 65060AB4 D9ACDD5B 337C4F8E

C2F918EE B4FEAD50 B3541BED 171BB5F9

0203

010001

Set the authentication mode for SSH user **huawei01** to password authentication and test the login.

#Set the authentication mode for the SSH user to password authentication.

[R1]

#Check the global configuration on the SSH server.

[R1]display ssh server status

SSH version :1.99

SSH connection timeout :60 seconds

SSH server key generating interval :0 hours

SSH Authentication retries :3 times

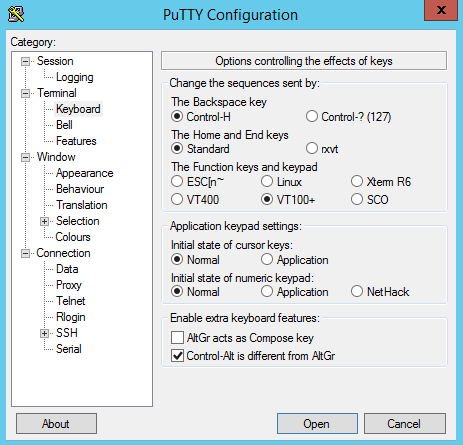
SFTP Server :Disable

Stelnet server :Disable

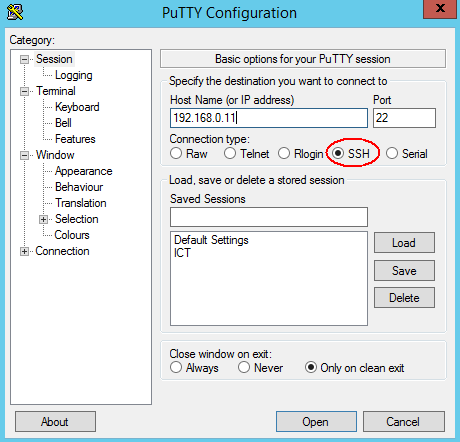
#Use a client (such as PuTTY) to perform a login test.

Set the PuTTY keyboard and session.

PuTTY keyboard settings



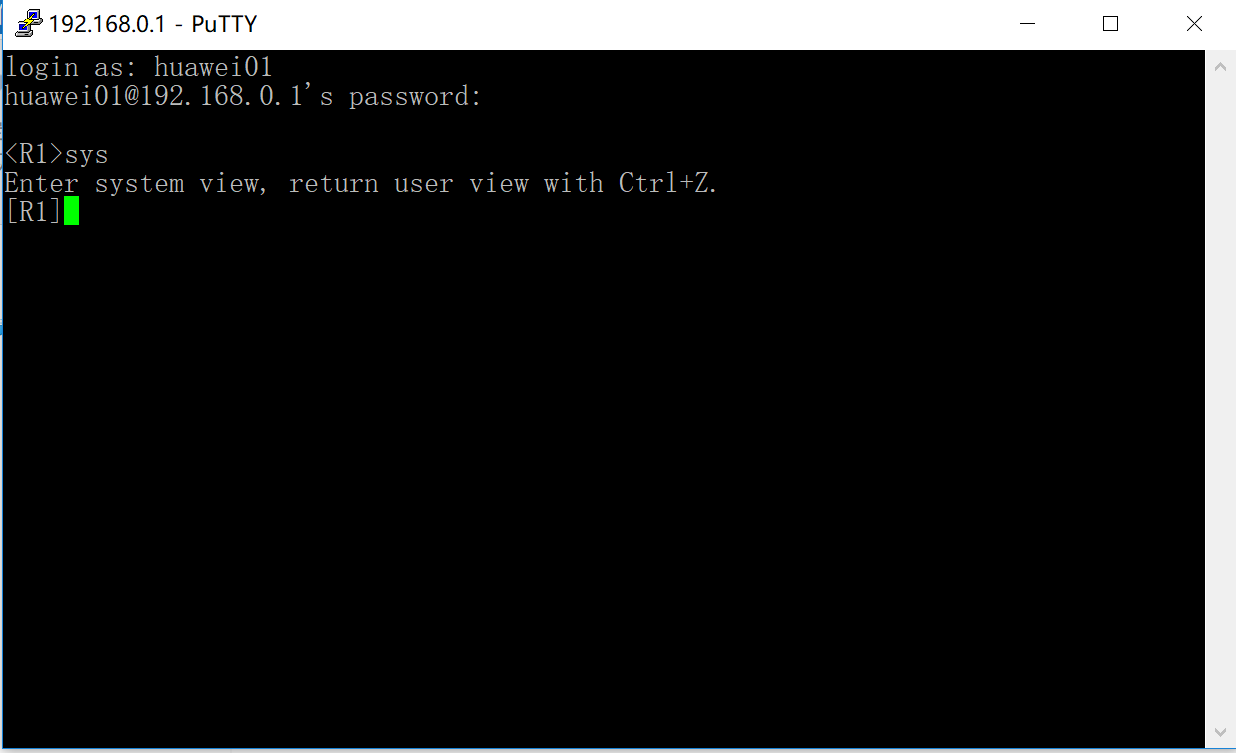
PuTTY session settings (SSH login)



Click **Open**. During the first login, in the security warning dialog box that is displayed, click **Yes**.

Enter the user name and password on the login page that is displayed.

PuTTY login page (STelnet)



Run the **display ssh server session** command to check information about sessions between the SSH server and client.

[R1]display ssh server session

-------------------------------------------------------------------------------------

Conn Ver Encry State Auth-type Username

-------------------------------------------------------------------------------------

VTY 0 2.0 AES run password huawei01

-------------------------------------------------------------------------------------

Run the **display ssh user-information** *username* command to check information about the specified SSH user. In the command, *username* is the user name displayed in the previous step. In this example, the user name is **huawei01**.

[R1]display ssh user-information huawei

------------------------------------------------------------------------------------

Username Auth-type User-public-key-name

------------------------------------------------------------------------------------

huawei01 password null

------------------------------------------------------------------------------------

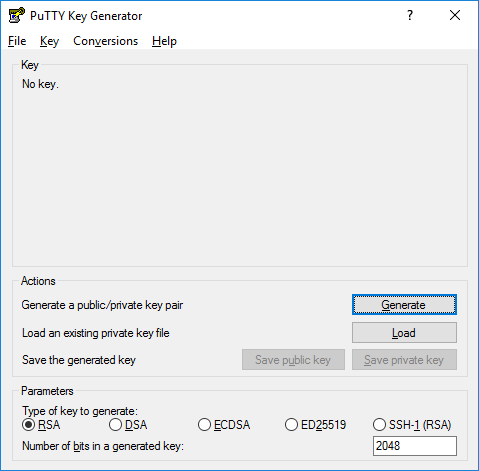
Set the authentication mode for SSH user **huawei02** to RSA authentication and test the login.

#Set the authentication mode for SSH user **huawei02** to RSA authentication.

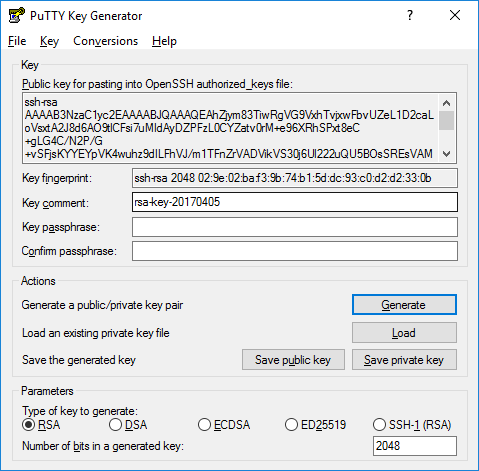
[R1]

#Run **puttygen.exe** on the remote maintenance terminal to generate the public key and private key files for future use. As shown in Figure 1-4, select **RSA** and click **Generate** to enter the key generation state. You can move the cursor around the blank area to check the generation of the keys.

PuTTYgen key generation settings



PuTTYgen key pair generation

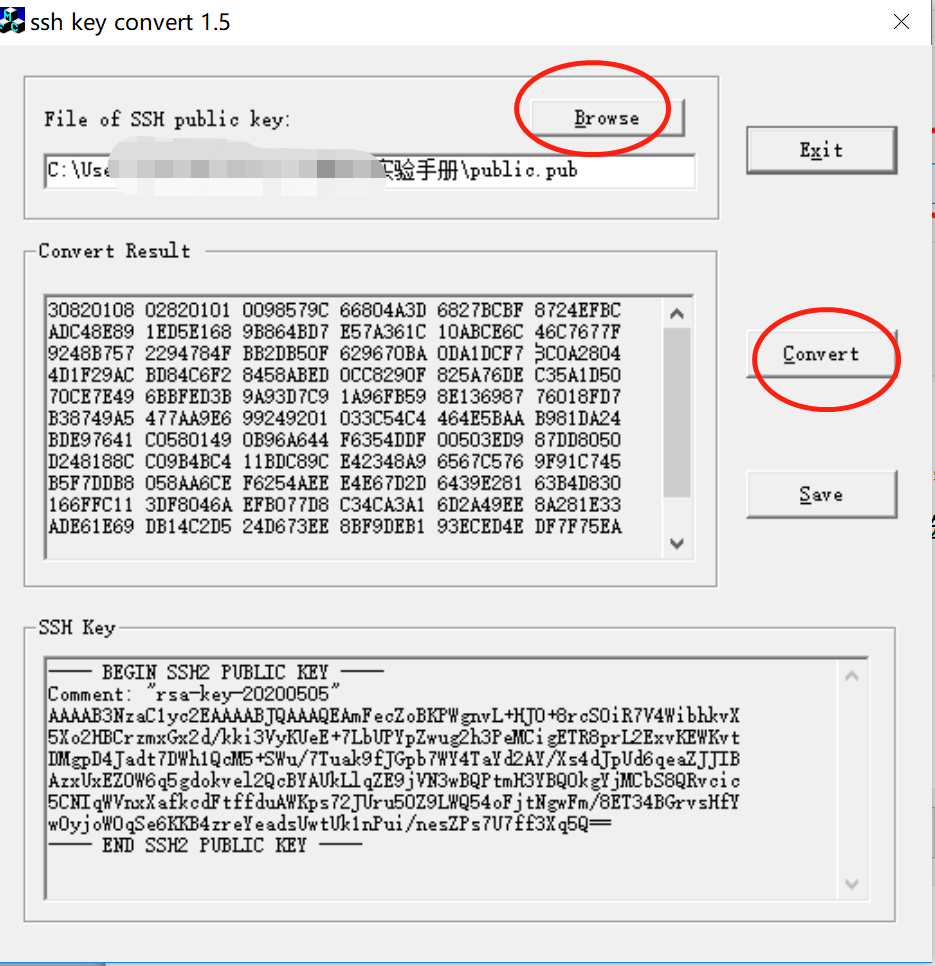


After the keys are generated, click **Save Public Key** to save the file as **public.pub**. Then click **Save Private Key**. In the dialog box that is displayed as shown in **错误!未找到引用源。**, click **Yes** to save the file as **private.ppk**.

#Run **sshkey.exe** on the remote maintenance terminal. Convert the generated public key to the character string required by the device.

Open the generated public key file **public.pub** and click **Convert** to check the original and converted public keys, as shown in Figure 1-7.

Converting the public key of the client



#On R1, edit and enter the RSA public key generated on the remote maintenance terminal. That is, copy the hexadecimal character string converted in Figure 1-7 as the RSA public key character string.

[R1]rsa peer-public-key huawei02

[R1-rsa-public-key]public-key-code begin

[R1-rsa-key-code]30820108 02820101 0098579C 66804A3D 6827BCBF 8724EFBC

[R1-rsa-key-code]ADC48E89 1ED5E168 9B864BD7 E57A361C 10ABCE6C 46C7677F

[R1-rsa-key-code]9248B757 2294784F BB2DB50F 629670BA 0DA1DCF7 8C0A2804

[R1-rsa-key-code]4D1F29AC BD84C6F2 8458ABED 0CC8290F 825A76DE C35A1D50

[R1-rsa-key-code]70CE7E49 6BBFED3B 9A93D7C9 1A96FB59 8E136987 76018FD7

[R1-rsa-key-code]B38749A5 477AA9E6 99249201 033C54C4 464E5BAA B981DA24

[R1-rsa-key-code]BDE97641 C0580149 0B96A644 F6354DDF 00503ED9 87DD8050

[R1-rsa-key-code]D248188C C09B4BC4 11BDC89C E42348A9 6567C576 9F91C745

[R1-rsa-key-code]B5F7DDB8 058AA6CE F6254AEE E4E67D2D 6439E281 63B4D830

[R1-rsa-key-code]166FFC11 3DF8046A EFB077D8 C34CA3A1 6D2A49EE 8A281E33

[R1-rsa-key-code]ADE61E69 DB14C2D5 24D673EE 8BF9DEB1 93ECED4E DF7F75EA

[R1-rsa-key-code]E5020125

[R1-rsa-key-code]public-key-code end

[R1-rsa-public-key]peer-public-key end

#Bind the RSA public key of the STelnet client to SSH user **huawei02** on R1.

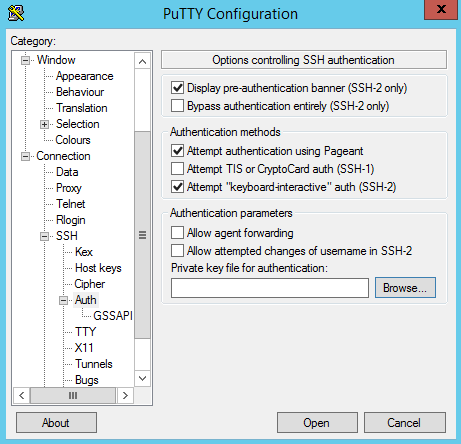
[R1]

#Test the login on the remote maintenance terminal.

Log in to the device using PuTTY, enter the device IP address, select the SSH protocol, and set keyboard parameters. The parameters are the same as those in password authentication mode, as shown in Figure 1-2 and Figure 1-3.

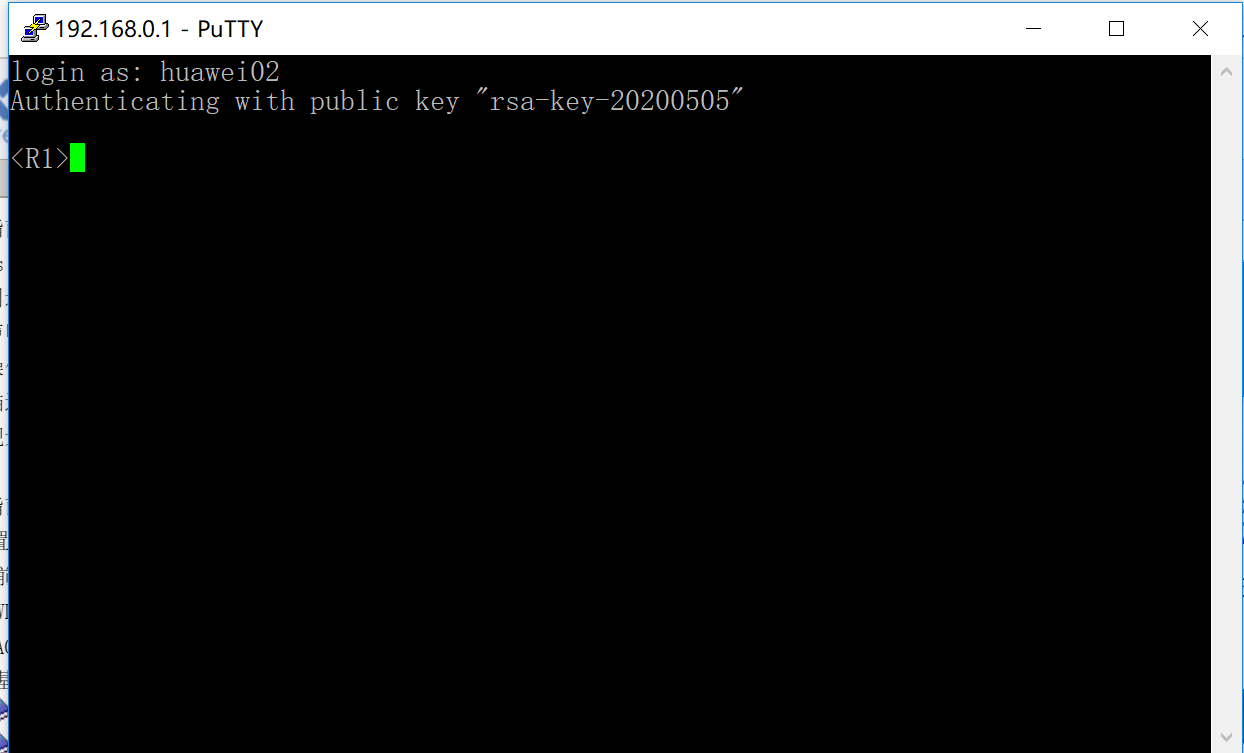
On PuTTY, choose **SSH** > **Authentication**. In the displayed dialog box, click **Browse** and select the private key file **private.ppk** saved in Step 7.

PuTTY STelnet login (RSA authentication)



Click **Open**. The login page is displayed. Enter user name **huawei02** to log in to the device, as shown in Figure 1-9.

Logging in to the device through STelnet using PuTTY (RSA authentication)



Run the **display ssh server session** command to check information about sessions between the SSH server and client.

[R1]display ssh server session

-------------------------------------------------------------------------------------

Conn Ver Encry State Auth-type Username

-------------------------------------------------------------------------------------

VTY 0 2.0 AES run rsa huawei02

-------------------------------------------------------------------------------------

Run the **display ssh user-information** *username* command to check information about the specified SSH user. In the command, *username* is the user name displayed in the previous step. In this example, the user name is **huawei02**.

[R1]display ssh user-information

-------------------------------------------------------------------------------

Username Auth-type User-public-key-name

-------------------------------------------------------------------------------

huawei02 rsa huawei02

-------------------------------------------------------------------------------

----End