**Telnet 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.



# Telnet Login and Management

## Background

During O&M, console login requires administrators to arrive at the site to log in to a device through the console port. To ease O&M, enterprises require that administrators remotely manage the device. Telnet login is then used to meet this requirement. In this exercise, an administrator sets up a Telnet login environment through the console port, configures password authentication and AAA authentication, and tests the login.

## Objectives

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

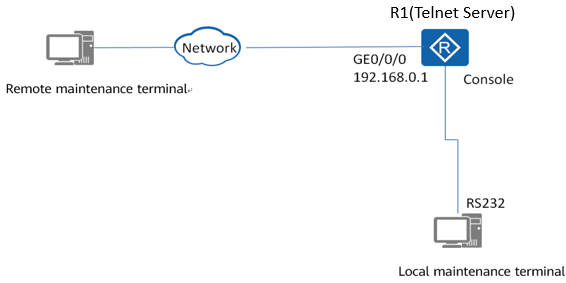
Understand the remote login process.

Configure Telnet login in password authentication mode.

Configure Telnet login in AAA local authentication mode.

## 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 the device name and an IPv4 address.
3. Configure the Telnet login environment in password authentication mode and test the login.
4. Configure the Telnet login environment in AAA local authentication mode 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 Management" in the previous exercise.

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

<Huawei>system-view

[Huawei]sysname R1

[R1]interface GigabitEthernet 0/0/0

[R1-GigabitEthernet0/0/0]ip address 192.168.0.1 24

Configure the Telnet login environment in password authentication mode and test the login.

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

[R1]

#Enter the VTY user interface view, set the authentication mode to password authentication, and set the password to **huawei123**.

[R1]user-interface vty 0 14

[R1-ui-vty0-14]

#Set the user privilege level to 0 and configure VTY user interfaces to support Telnet.

[R1-ui-vty0-14]

[R1-ui-vty0-14]

#Set the IP address of the remote maintenance terminal to be in the same segment as the IP address of GE0/0/0 on R1, for example, 192.168.0.11. Run the **telnet 192.168.0.1** command at the command prompt, and enter the correct user name **huawei123** to log in to R1. (Note that the cursor does not move when you enter the password.)

C:\Users>telnet 192.168.0.1

Login authentication

Password:

<R1>

#Run the **system-view** command on the remote maintenance terminal. The command, however, cannot be executed.

<R1>system-view

^

Error: Unrecognized command found at '^' position.

#On the local maintenance terminal, set the password of the super user to **huawei@123**. By default, the super user's privilege level is 3.

[R1]

#On the remote maintenance terminal, run the **super** command to increase the user privilege level, and then run the **system-view** command again.

<R1>super

Password:

Now user privilege is level 3, and only those commands whose level is

equal to or less than this level can be used.

Privilege note: 0-VISIT, 1-MONITOR, 2-SYSTEM, 3-MANAGE

<R1>system-view

Enter system view, return user view with Ctrl+Z.

[R1]

Configure the Telnet login environment in AAA local authentication mode and test the login.

#Enter the AAA view, configure a local user for Telnet login, set the user name to **huawei**, password to **huawei123**, and user privilege level to 0.

[R1] aaa

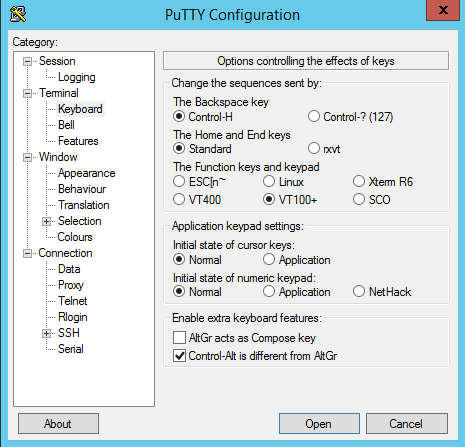
#Set the authentication mode to AAA authentication in the VTY user interface view.

[R1]user-interface vty 0 14

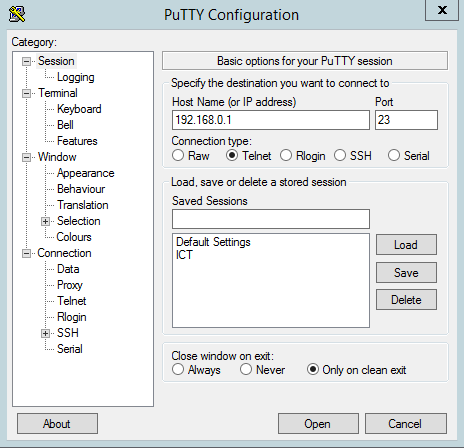
[R1-ui-vty0-14]

#On the remote maintenance terminal, start the third-party software (such as PuTTY) to configure keyboard parameters and session parameters. When configuring keyboard parameters, select **Control-H** for **The Backspace key** and **VT100+** for **The Function keys and keypad**.

PuTTY keyboard settings

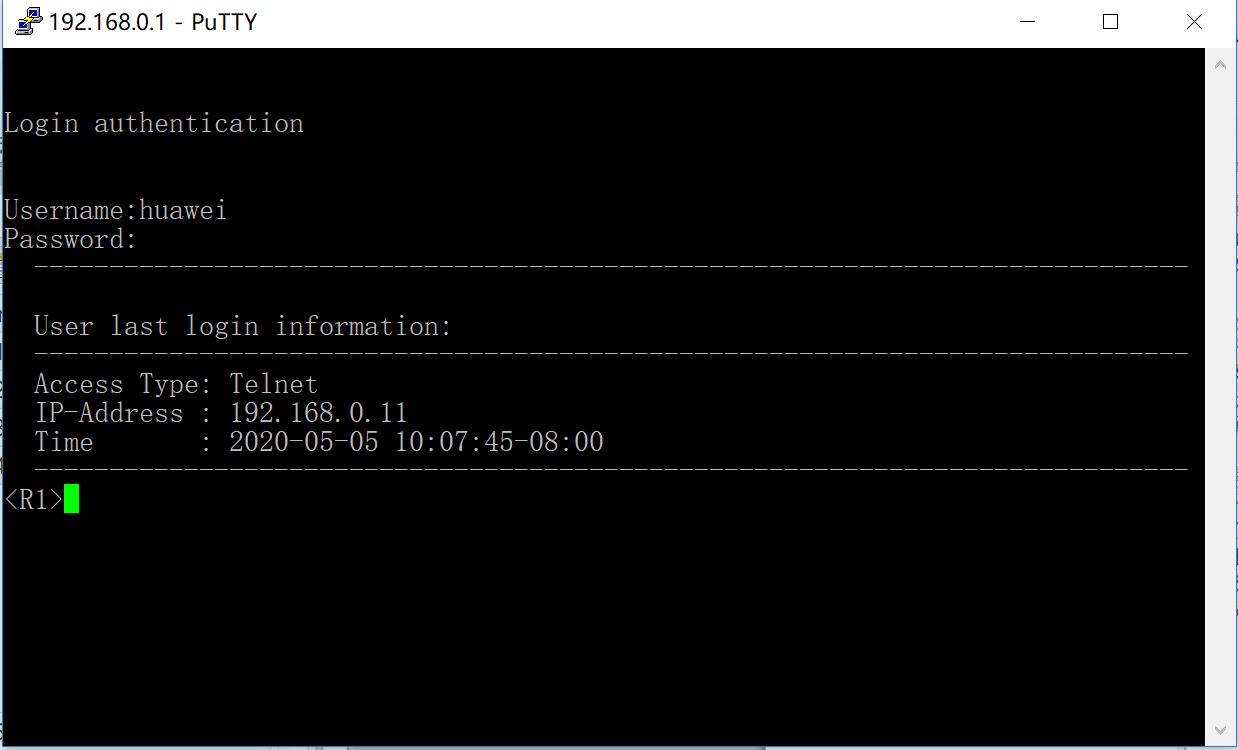


PuTTY session settings



#Click **Open**. In the displayed CLI, enter the user name **huawei** and password **huawei123** to log in.

Entering the user name and password for login using PuTTY



#After the login is successful, run the **system-view** command. The command, however, cannot be executed because the default user privilege level is 0.

<R1>system-view

^

Error: Unrecognized command found at '^' position.

#Run the **super** command to increase the user privilege level, and then run the **system-view** command again.

<R1>super

Password:

Now user privilege is level 3, and only those commands whose level is

equal to or less than this level can be used.

Privilege note: 0-VISIT, 1-MONITOR, 2-SYSTEM, 3-MANAGE

<R1>system-view

Enter system view, return user view with Ctrl+Z.

[R1]

Clearing the console login password sets the authentication mode for console login to non-authentication. After the device restarts, you can directly log in to the device without entering the user name and password. To ensure console port security, it is recommended that you change the authentication mode for console login to AAA authentication after logging in to the device.

----End