**Establishing Local AAA Solutions**

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.



# Establishing Local AAA Solutions

## Background

Authentication, authorization, and accounting (AAA) provides a management mechanism for network security.

AAA provides the following functions:

Authentication: verifies whether users are permitted to access the network.

Authorization: authorizes users to use particular services.

Accounting: records the network resources used by users.

Users can use one or more security services provided by AAA. For example, if a company wants to authenticate employees that access certain network resources, the network administrator only needs to configure an authentication server. If the company also wants to record operations performed by employees on the network, an accounting server is needed.

In summary, AAA authorizes users to access specific resources and records user operations. AAA is widely used because it features good scalability and facilitates centralized user information management. AAA can be implemented using multiple protocols. RADIUS is most frequently used in actual scenarios.

In this lab activity, you will configure local AAA to manage and control resources for remote Telnet users.

## Objectives

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

Learn how to configure local AAA

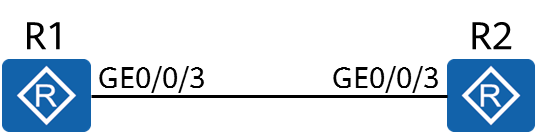
Learn how to create a domain

Learn how to create a local user

Understand domain-based user management

## Topology

Lab Topology



R1 functions as a client, and R2 functions as a network device. Access to the resources on R2 needs to be controlled. Therefore, you need to configure local AAA authentication on R1 and R2 and manage users based on domains, and configure the privilege level for authenticated users.

## Implementation

### Roadmap

1. Configure an AAA scheme.
2. Create a domain and apply the AAA scheme to the domain.
3. Configure local users.

### Procedure

Complete basic device configuration.

# Name R1 and R2.

The details are not provided here.

# Configure IP addresses for R1 and R2.

[R1]interface GigabitEthernet 0/0/3

[R1-GigabitEthernet0/0/3]ip address 10.0.12.1 24

[R2]interface GigabitEthernet 0/0/3

[R2-GigabitEthernet0/0/3]ip address 10.0.12.2 24

Configure an AAA scheme.

# Configure authentication and authorization schemes.

[R2-aaa]aaa

*Enter the AAA view.*

[R2-aaa]

*Create an authentication scheme named datacom.*

[R2]

*Set the authentication mode to local authentication.*

[R2]

*Create an authorization scheme named datacom.*

[R2]

*Set the authorization mode to local authorization.*

[R2]

A device functioning as an AAA server is called a local AAA server, which can perform authentication and authorization, but not accounting.

The local AAA server requires a local user database, containing the user name, password, and authorization information of local users. A local AAA server is faster and cheaper than a remote AAA server, but has a smaller storage capacity.

Create a domain and apply the AAA scheme to the domain.

[R2]aaa

The devices manage users based on domains. A domain is a group of users and each user belongs to a domain. The AAA configuration for a domain applies to the users in the domain. Create a domain named datacom.

[R2]

*The authentication scheme named datacom is used for users in the domain.*

[R2]

*The authorization scheme named datacom is used for users in the domain.*

Configure local users.

# Create a local user and password.

[R2-aaa]local-user hcia@datacom password cipher HCIA-Datacom

Info: Add a new user.

If the user name contains a delimiter of at sign (@), the character string before the at sign is the user name and the character string following the at sign is the domain name. If the value does not contain the at sign, the entire character string represents the user name and the domain name is the default one.

# Configure the parameters for the local user, such as access type and privilege level.

[R2-aaa]

The **local-user service-type** command configures the access type for a local user. After you specify the access type of a user, the user can successfully log in only when the configured access type is used. If the access type is set to telnet, the user cannot access the device through a web page. Multiple access types can be configured for a user.

[R2-aaa]

The privilege level of the local user is specified. Only commands within the specified privilege level or a lower level are available for a user.

Enable the telnet function on R2.

[R2]

*The Telnet server function is enabled on the device. This function is enabled by default on some devices.*

[R2]user-interface vty 0 4

[R2-ui-vty0-4]

The **authentication-mode** command configures an authentication mode for accessing the user interface. By default, the user authentication mode of the VTY user interface is not configured. An authentication mode must be configured for the login interface. Otherwise, users will not be able to log in to the device.

Verify the configuration.

# Telnet R2 from R1.

<R1>telnet 10.0.12.2

Press CTRL\_] to quit telnet mode

Trying 10.0.12.2 ...

Connected to 10.0.12.2 ...

Login authentication

Username:hcia@datacom

Password:

<R2>

*R1 has logged in to R2.*

# Display the online users on R2.

[R2]display users

User-Intf Delay Type Network Address AuthenStatus AuthorcmdFlag

129 VTY 0 00:02:43 **TEL** **10.0.12.1**  pass

Username : hcia@datacom

**----End**

* 1. **Verification**

The details are not provided here.