AAA Principles and Configuration



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.



Contents

[1 AAA Principles and Configuration 1](#_Toc59716859)

[1.1 Foreword 1](#_Toc59716860)

[1.2 Objectives 1](#_Toc59716861)

[1.3 AAA Overview 2](#_Toc59716862)

[1.3.1 Basic Concepts of AAA 2](#_Toc59716863)

[1.3.2 Common AAA Architecture 2](#_Toc59716864)

[1.3.3 Authentication 3](#_Toc59716865)

[1.3.4 Authorization 4](#_Toc59716866)

[1.3.5 Accounting 5](#_Toc59716867)

[1.3.6 AAA Implementation Protocol - RADIUS 6](#_Toc59716868)

[1.3.7 Common AAA Application Scenarios 8](#_Toc59716869)

[1.4 AAA Configuration 9](#_Toc59716870)

[1.4.1 AAA Configuration 9](#_Toc59716871)

[1.4.2 AAA Configuration Examples 10](#_Toc59716872)

[1.4.3 Configuration Verification 10](#_Toc59716873)

[1.5 Summary 12](#_Toc59716874)

[1.6 Quiz 13](#_Toc59716875)

# AAA Principles and Configuration

## Foreword

User management is one of the most basic security management requirements for   
any network.

Authentication, authorization, and accounting (AAA) is a management framework that provides a security mechanism for authorizing some users to access specified resources and recording the operations of these users. AAA is widely used because of its good scalability and easy implementation of centralized management of user information. AAA can be implemented through multiple protocols. In actual applications, the Remote Authentication Dial-In User Service (RADIUS) protocol is the most commonly used to implement AAA.

This course describes the basic concepts, implementation, basic configurations, and typical application scenarios of AAA.

## Objectives

On completion of this course, you will be able to:

Understand the fundamentals of AAA.

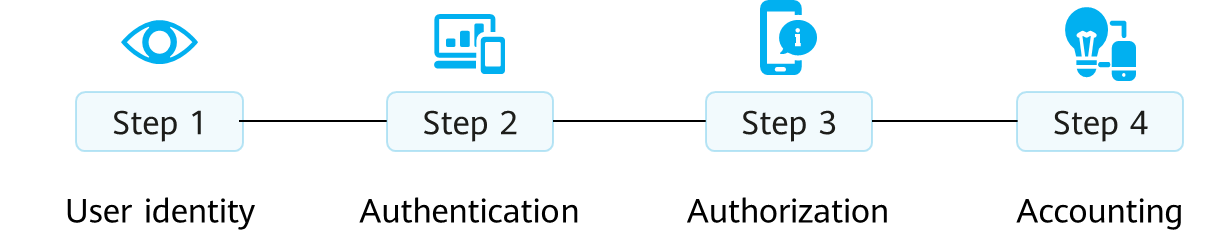
Describe the application scenarios of AAA.

Understand the fundamentals of RADIUS.

Get familiar with the basic configurations of AAA.

## AAA Overview

### Basic Concepts of AAA



AAA

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

Process of AAA:

1. User identity:Identifies users by information such as the account and password.
2. Authentication:Identifies and authenticates users who attempt to access resources.
3. Authorization:Determines whether the access is granted authorization.
4. Accounting:Checks and records access information.

Authentication: determines which users can access the network.

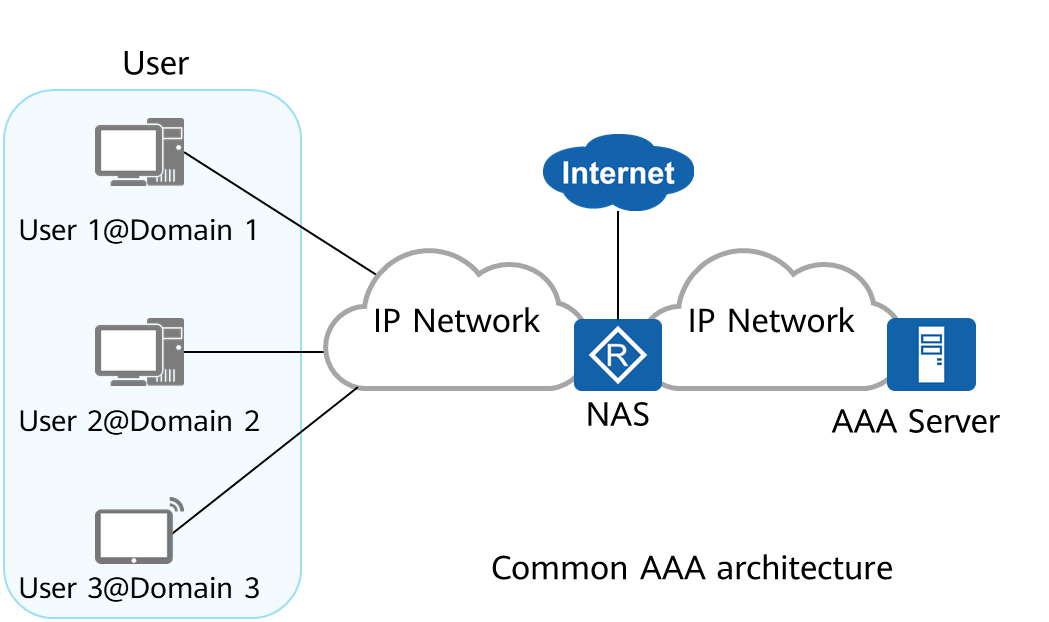
Authorization: authorizes users to access specific services.

Accounting: records network resource utilization.

The Internet service provider (ISP) needs to authenticate the account and password of a home broadband user before allowing the user to access the Internet. In addition, the ISP records the online duration or traffic of the user. This is the most common application scenario of the AAA technology.

### Common AAA Architecture

A common AAA architecture includes the user, network access server (NAS), and AAA server.



AAA architecture

The NAS collects and manages user access requests in a centralized manner.

Multiple domains are created on the NAS to manage users. Different domains can be associated with different AAA schemes, which include the authentication scheme, authorization scheme, and accounting scheme.

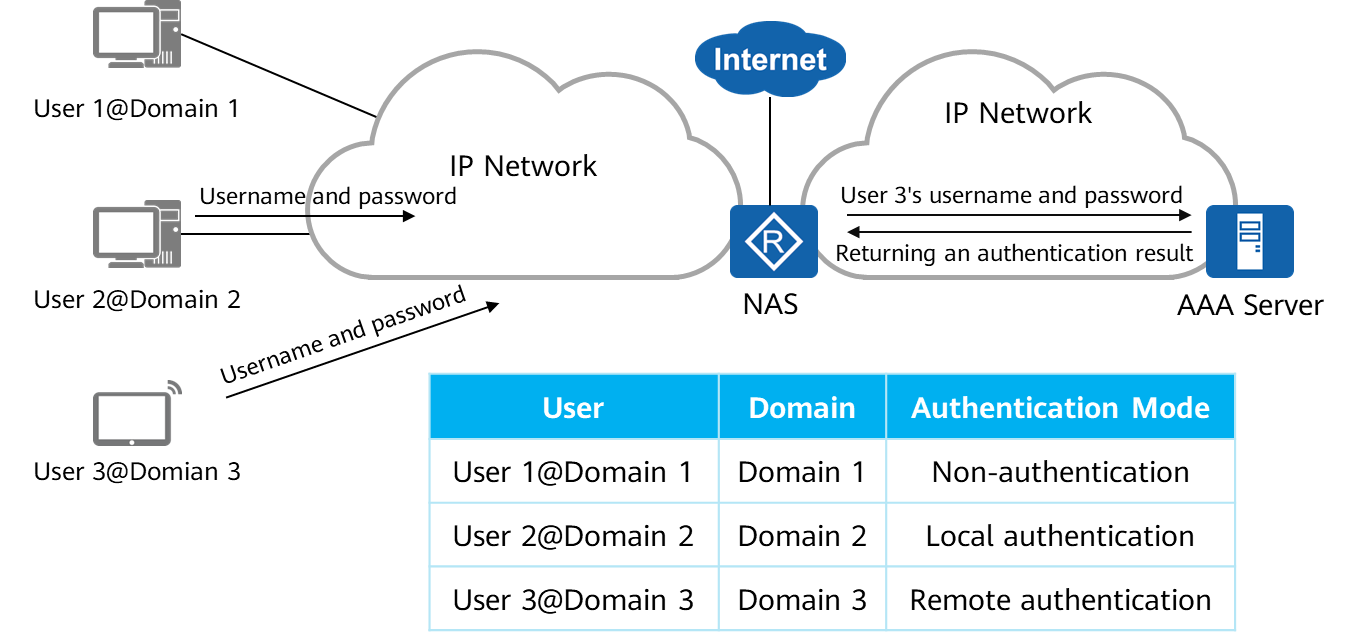
When receiving a user access request, the NAS determines the domain to which the user belongs based on the username and performs user management and control based on the AAA schemes configured for the domain.

The NAS manages users based on domains. Each domain can be configured with different authentication, authorization, and accounting schemes to perform authentication, authorization, and accounting for users in the domain.

Each user belongs to a domain. The domain to which a user belongs is determined by the character string following the domain name delimiter @ in the user name. For example, if the user name is user 1@domain 1, the user belongs to domain 1. If the user name does not end with @, the user belongs to the default domain.

### Authentication

AAA supports the following authentication modes: non-authentication, local authentication, and remote authentication.



Authentication

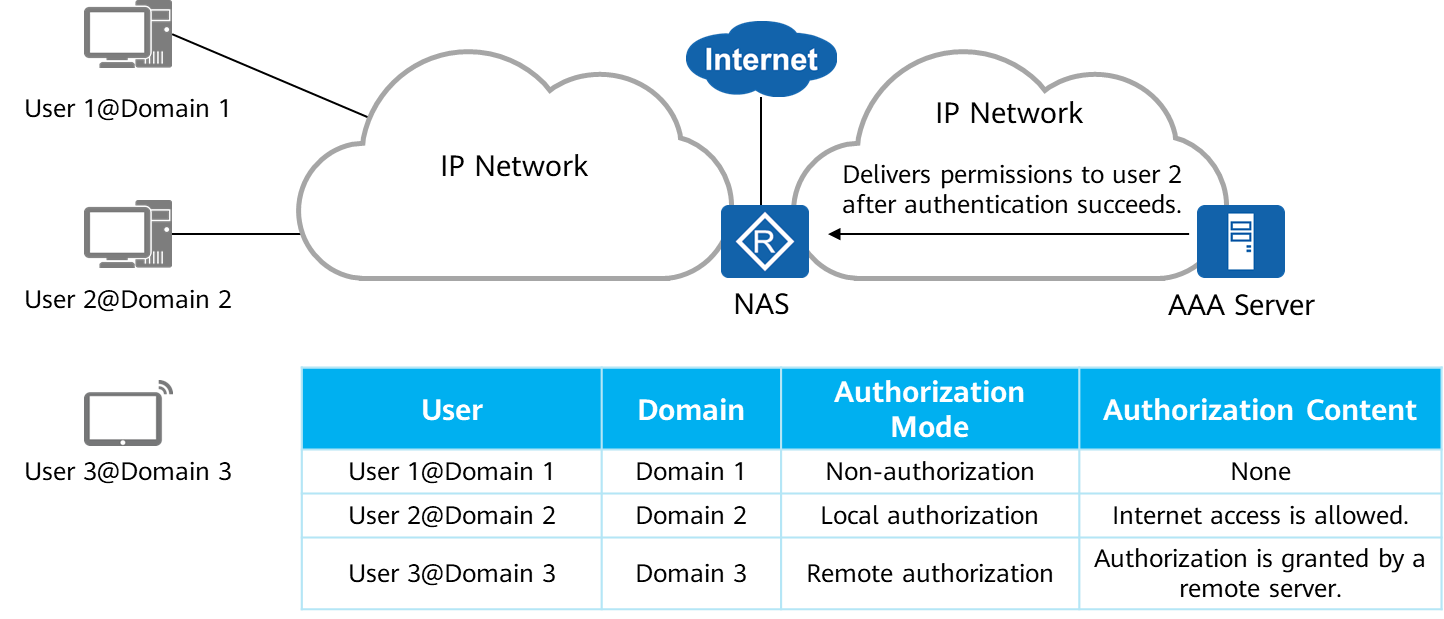
AAA supports three authentication modes:

* Non-authentication: Users are fully trusted and their identities are not checked. This authentication mode is seldom used for security purposes.
* Local authentication: Local user information (including the username, password, and attributes) is configured on the NAS. In this case, the NAS functions as the AAA server. Local authentication features fast processing and low operational costs. The disadvantage is that the amount of stored information is limited by device hardware. This authentication mode is often used to manage login users, such as Telnet and FTP users.
* Remote authentication: User information (including the username, password, and attributes) is configured on the authentication server. Remote authentication can be implemented through RADIUS or HWTACACS. The NAS functions as a client to communicate with the RADIUS or HWTACACS server.

### Authorization

AAA supports the following authorization modes: non-authorization, local authorization, and remote authorization.

Authorization information includes the user group, VLAN ID, and ACL number.



Authorization

The AAA authorization function grants users the permission to access specific networks or devices. AAA supports the following authorization modes:

* Non-authorization: Authenticated users have unrestricted access rights on a network.
* Local authorization: Users are authorized based on the domain configuration on the NAS.
* Remote authorization: The RADIUS or HWTACACS server authorizes users.

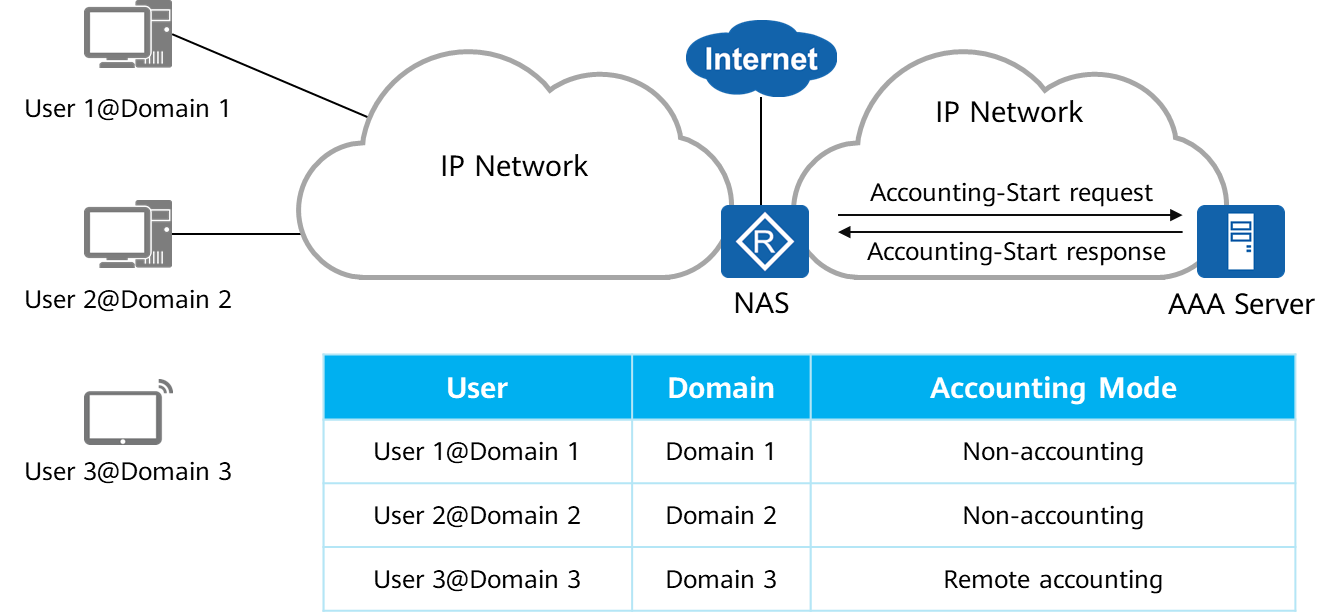
1. In HWTACACS authorization, all users can be authorized by the HWTACACS server.
2. RADIUS authorization applies only to the users authenticated by the RADIUS server. RADIUS integrates authentication and authorization. Therefore, RADIUS authorization cannot be performed singly.

When remote authorization is used, users can obtain authorization information from both the authorization server and NAS. The priority of the authorization information configured on the NAS is lower than that delivered by the authorization server.

### Accounting

The accounting function monitors the network behavior and network resource utilization of authorized users.

AAA supports two accounting modes: non-accounting and remote accounting.



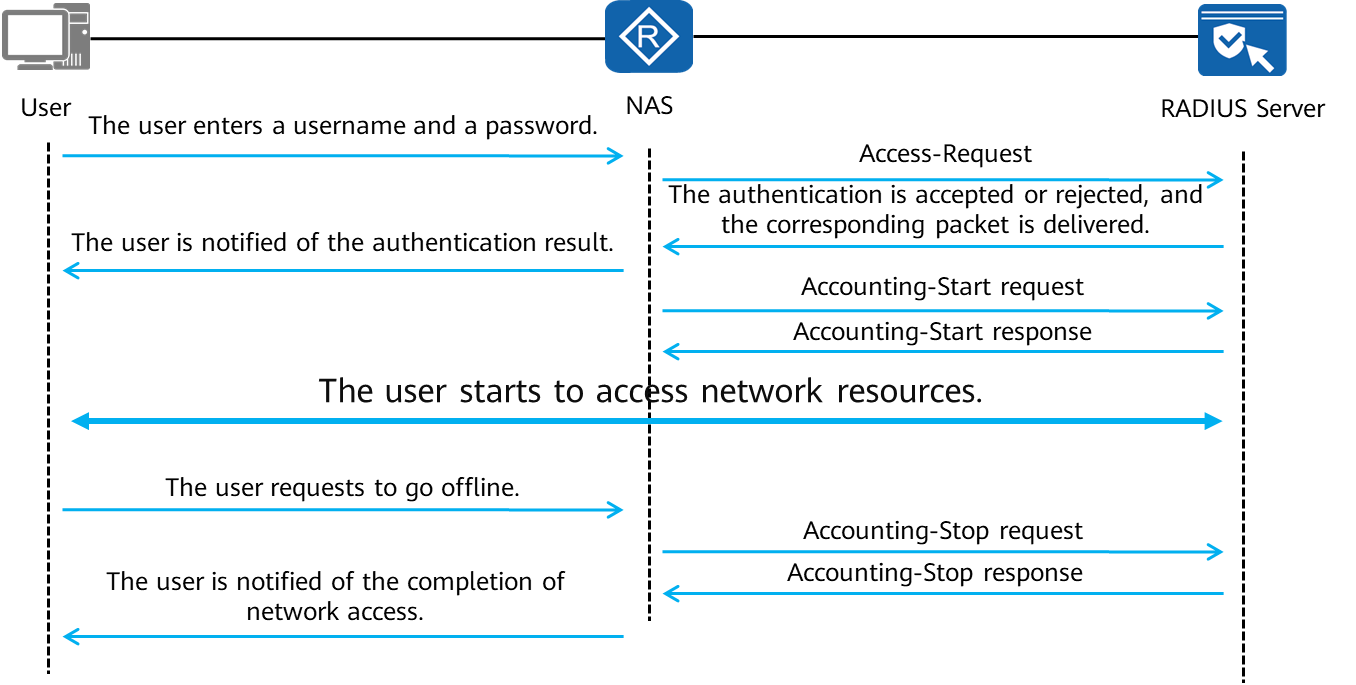
Accounting

AAA supports the following accounting modes:

* Non-accounting: Users can access the Internet for free, and no activity log is generated.
* Remote accounting: Remote accounting is performed through the RADIUS server or HWTACACS server.

### AAA Implementation Protocol - RADIUS

Of the protocols that are used to implement AAA, RADIUS is the most commonly used.



Process of RADIUS

Of the protocols that are used to implement AAA, RADIUS is the most commonly used. RADIUS is a distributed information exchange protocol based on the client/server structure. It implements user authentication, accounting, and authorization.

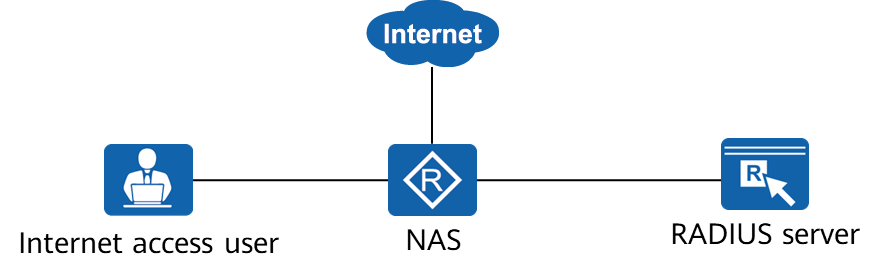
Generally, the NAS functions as a RADIUS client to transmit user information to a specified RADIUS server and performs operations (for example, accepting or rejecting user access) based on the information returned by the RADIUS server.

RADIUS servers run on central computers and workstations to maintain user authentication and network service access information. The servers receive connection requests from users, authenticate the users, and send the responses (indicating that the requests are accepted or rejected) to the clients. RADIUS uses the User Datagram Protocol (UDP) as the transmission protocol and uses UDP ports 1812 and 1813 as the authentication and accounting ports, respectively. RADIUS features high real-time performance. In addition, the retransmission mechanism and standby server mechanism are also supported, providing good reliability.

The message exchange process between the RADIUS server and client is as follows:

* When a user accesses the network, the user initiates a connection request and sends the username and password to the RADIUS client (NAS).
* The RADIUS client sends an authentication request packet containing the username and password to the RADIUS server.
* If the request is valid, the RADIUS server completes authentication and sends the required authorization information to the RADIUS client. If the request is invalid, the RADIUS server sends the authorization failure information to the RADIUS client.
* The RADIUS client notifies the user of whether authentication is successful.
* The RADIUS client permits or rejects the user according to the authentication result. If the user is permitted, the RADIUS client sends an Accounting-Request (Start) packet to the RADIUS server.
* The RADIUS server sends an Accounting-Response (Start) packet to the RADIUS client and starts accounting.
* The user starts to access network resources.
* When a user does not want to access network resources, the user sends a logout request to stop accessing network resources.
* The RADIUS client sends an Accounting-Request (Stop) packet to the RADIUS server.
* The RADIUS server sends an Accounting-Response (Stop) packet to the RADIUS client and stops accounting.
* The RADIUS client notifies the user of the processing result, and the user stops accessing network resources.

### Common AAA Application Scenarios



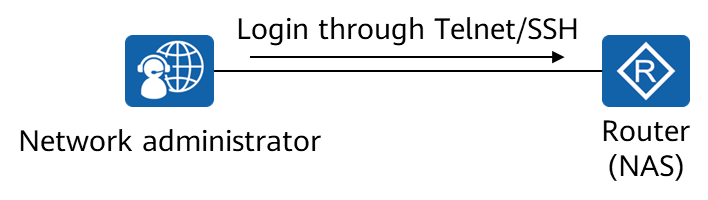
AAA for Internet Access Users Through RADIUS

AAA schemes are configured on the NAS to implement interworking between the NAS and RADIUS server.

After the user enters a username and a password on the client, the NAS sends the username and password to the RADIUS server for authentication.

If the authentication succeeds, the user is granted the Internet access permission.

The RADIUS server can record the user's network resource utilization during Internet access.



Local Authentication and Authorization for Administrative Users

After local AAA schemes are configured on Router, Router compares the username and password of the network administrator with the locally configured username and password when the network administrator logs in to Router.

After the authentication succeeds, Router grants certain administrator permissions to the network administrator.

## AAA Configuration

### AAA Configuration

* Enter the AAA view.

[Huawei] **aaa**

Exit the system view and enter the AAA view.

* Create an authentication scheme.

[Huawei-aaa] **authentication-scheme** *authentication-scheme-name*

Create an authentication scheme and enter the authentication scheme view.

[Huawei-aaa-authentication-scheme-name] **authentication-mode { hwtacacs | local | radius }**

Set the authentication mode to local authentication. By default, the authentication mode is local authentication.

The authorization-scheme authorization-scheme-name command configures an authorization scheme for a domain. By default, no authorization scheme is applied to a domain.

The authentication-mode { hwtacacs | local | radius } command configures an authentication mode for the current authentication scheme. By default, local authentication is used.

* Create a domain and bind an authentication scheme to the domain.

[Huawei-aaa] **domain** *domain-name*

Create a domain and enter the domain view.

[Huawei-aaa-domain-name] **authentication-scheme** *authentication-scheme-name*

Bind the authentication scheme to the domain.

* Create a user.

[Huawei-aaa] **local-user** *user-name* **password cipher** password

Create a local user and configure a password for the local user.

1. If the username contains a delimiter "@", the character before "@" is the username and the character after "@" is the domain name.
2. If the value does not contain "@", the entire character string represents the username and the domain name is the default one.

* Configure a user access type.

[Huawei-aaa] **local-user user-name service-type { { terminal | telnet | ftp | ssh | snmp | http } | ppp | none }**

Configure the access type of the local user. By default, all access types are disabled for a local user.

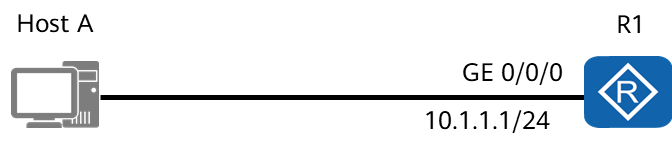
* Configure a user level.

[Huawei-aaa] **local-user** *user-name* **privilege level** *level*

Specify the permission level of the local user.

### AAA Configuration Examples

After a user password and a user level are configured on R1, host A can use the configured username and password to remotely log in to R1.



DIAdiagram of AAA configuration

The command is follow：

[R1]aaa

[R1-aaa]local-user huawei password cipher huawei123

[R1-aaa]local-user huawei service-type telnet

[R1-aaa]local-user huawei privilege level 0

[R1]user-interface vty 0 4

[R1-ui-vty0-4]authentication-mode aaa

### Configuration Verification

In AAA, each domain is associated with an authentication scheme, an authorization scheme, and an accounting scheme. In this example, the default domain is used.

[R1]display domain name default\_admin

Domain-name: default\_admin

Domain-state: Active

Authentication-scheme-name: default

Accounting-scheme-name: default

Authorization-scheme-name: -

Service-scheme-name: -

RADIUS-server-template: -

HWTACACS-server-template: -

User-group: -

The display domain [ name domain-name ]command displays the configuration of a domain.

If the value of Domain-state is Active, the domain is activated.

If the username does not end with @, the user belongs to the default domain. Huawei devices support the following default domains:

* The default domain is for common users.
* The default\_admin domain is the default domain for administrators.

After the user properly logs in and logs out, you can view the user record.

[R1]display aaa offline-record all

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

User name: huawei

Domain name: default\_admin

User MAC: 00e0-fc12-3456

User access type: telnet

User IP address: 10.1.1.2

User ID: 1

User login time: 2019/12/28 17:59:10

User offline time: 2019/12/28 18:00:04

User offline reason: user request to offline

The display aaa offline-record command displays user offline records.

## Summary

AAA improves enterprise network security and prevents unauthorized users from logging in to enterprise networks by authenticating the identities of enterprise employees and external users, authorizing accessible resources, and monitoring Internet access behavior.

* Authentication: determines which users can access the network.
* Authorization: authorizes users to access specific services.
* Accounting: records network resource utilization.

AAA technology can be implemented either locally or through a remote server.

Of the protocols that are used to implement AAA, RADIUS is the most commonly used.

## Quiz

1. (Single) AAA is a network security management mechanism. Which of the following functions cannot be provided by AAA? ( )
2. Authentication
3. Authorization
4. Accounting
5. Backup
6. (Multiple) What accounting modes does the AAA support? ( )
7. No accounting
8. Local accounting
9. Remote accounting
10. Manual accounting
11. (True or False) AAA configurations are as follows: ( )

[R1]aaa

[R1-aaa]local-user huawei password cipher huawei123

[R1-aaa]local-user huawei service-type telnet

[R1-aaa]local-user huawei privilege level 0

The user belongs to the huawei domain.

1. True
2. False
3. (True or False) By default, the authentication mode is local authentication, and no authorization scheme is bound to the default domain. ( )
4. True
5. False
6. (True or False) AAA can be implemented using multiple protocols, the most commonly used protocol is RADIUS. ( )
7. True
8. False
9. What authentication, authorization, and accounting modes are supported by AAA?
10. When a new common user is configured with local authentication but is not associated with a user-defined domain, which domain does the user belong to?