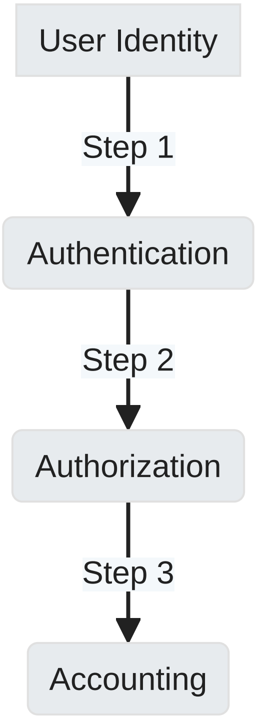
AAA Principles and Configuration

1 AAA Principles and Configuration

1.1 AAA Overview

1.1.1 AAA Concepts Overview



Note

AAA stands for Authentication, Authorization, and Accounting. It is a framework for controlling access to computer resources, enforcing policies,

> and providing the tracking of user activities.

1.1.1.1 Authentication

- Determines **who** can access the network.
- **Modes:**
  - `Non-authentication` : No identity check. Rarely used due to security concerns.
  - `Local authentication` : Credentials are stored on NAS. Quick but hardware-limited.
  - `Remote authentication` : Credentials on an external server (RADIUS/HWTACACS).

User	Domain	Authentication Mode
User1@Domain1	Domain1	Non-authentication
User2@Domain2	Domain2	Local authentication
User3@Domain3	Domain3	Remote authentication

1.1.1.2 Authorization

- Determines **what** users can do after they are authenticated.
- **Modes:**
  - `Non-authorization` : Unrestricted access after-authentication.
  - `Local authorization` : Permissions based on NAS domain config.
  - `Remote authorization` : Permissions granted by RADIUS/HWTACACS server.

User	Domain	Authorization Mode
User1@Domain1	Domain1	Non-authorization

User	Domain	Authorization Mode
User2@Domain2	Domain2	Local authorization
User3@Domain3	Domain3	Remote authorization

> In HWTACACS authorization, all users can be authorized by the HWTACACS server.

> RADIUS integrates authentication and authorization. Therefore, RADIUS authorization cannot be performed singly.

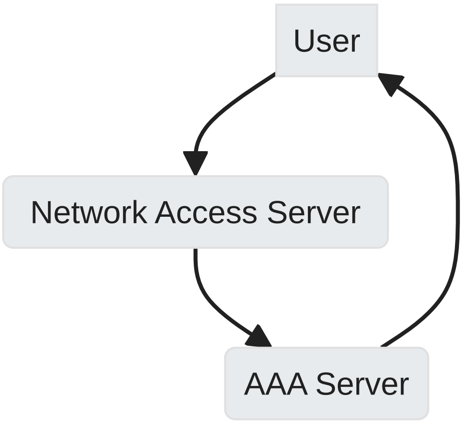
> When using remote authorization, the network access server (NAS) will prioritize the permissions given by the authorization server over its own settings.

1.1.1.3 Accounting

- Tracks network behavior and resource usage by authorized users.
- **Modes:**
  - `Non-accounting` : Free access with no logs.
  - `Remote accounting` : Activity tracking through RADIUS/HWTACACS server.

User	Domain	Accounting Mode
User1@Domain1	Domain1 Non-accounting	

1.1.2 Common AAA Architecture



> **Tip**
>
> Different domains on the NAS can be associated with different AAA schemes (authentication, authorization, accounting).

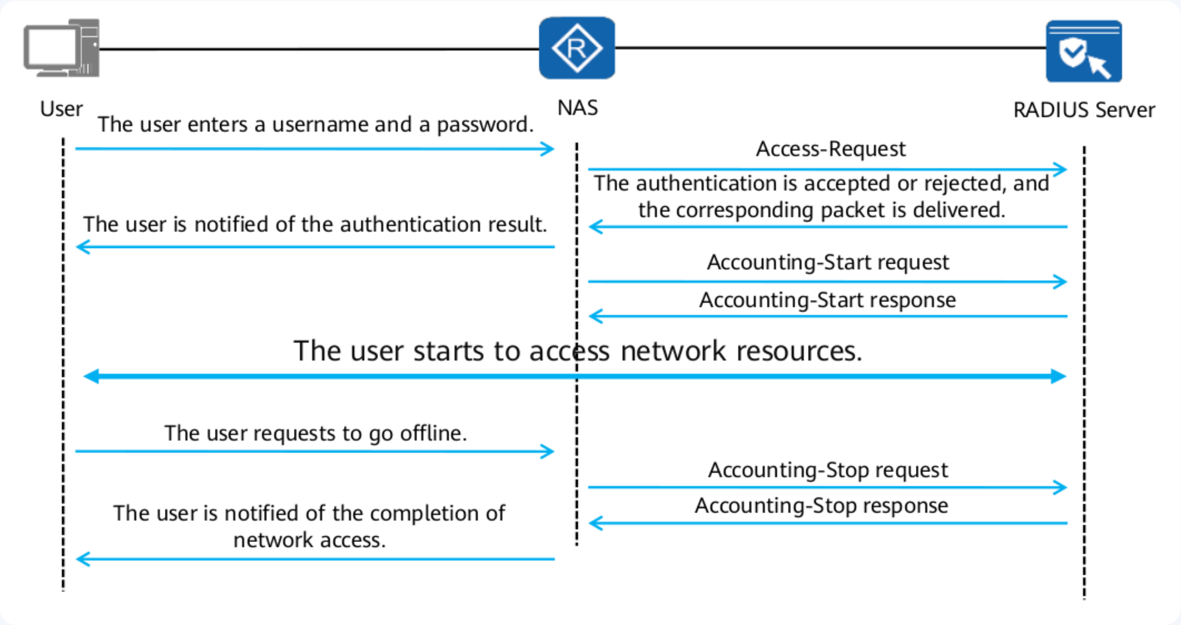
> **NAS (Network Attached Storage):** is a device that connects to a network, allowing multiple users and devices to store and access files from a central location.

1.1.3 RADIUS Implementation Protocol

The RADIUS protocol is commonly used for AAA implementations due to its distributed client/server model which supports user authentication, accounting, and authorization over UDP ports.

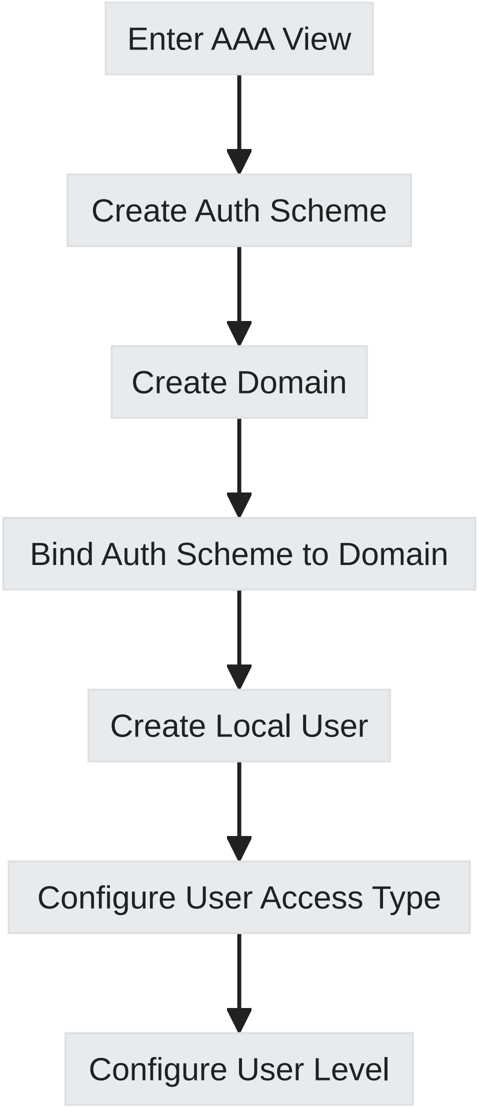
> **RADIUS,** which stands for Remote Authentication Dial-In User Service, is a protocol that helps manage access to network resources by verifying who is trying to connect (authentication), keeping track of what they're doing (accounting), and deciding what they are allowed to do (authorization). It operates over a network using UDP ports, which allows data to be sent quickly between the user's device and the server that checks their access rights.

> RADIUS uses UDP ports **1812** and 1813 **as** the authentication and accounting ports, respectively


User
NAS
RADIUS Server
The user enters a username and a password.
Access-Request
The authentication is accepted or rejected, and the corresponding packet is delivered.
The user is notified of the authentication result.
Accounting-Start request
Accounting-Start response
The user starts to access network resources.
The user requests to go offline.
Accounting-Stop request
Accounting-Stop response
The user is notified of the completion of network access.

1.2 AAA Configuration

1.2.1 Steps to Configure AAA



1.2.1.1 Step 1: Enter AAA View

Markdown

```
[Huawei] aaa
```

1.2.1.2 Step 2: Create Authentication Scheme

Markdown

```
[Huawei-aaa] authentication-scheme <scheme-name>
[Huawei-aaa-authentication-scheme-name] authentication-mode <mode>
```

- `<mode>`
  - hwtacacs
  - local
  - radius

> By default, the authentication mode is set to local.

1.2.1.3 Step 3: Create Domain and Bind Authentication Scheme

Markdown

```markdown
[Huawei-aaa] domain <domain-name>
[Huawei-aaa-domain-name] authentication-scheme <scheme-name>
```

> Bind your created authentication scheme to your new domain.

1.2.1.4 Step 4: Create Local User

Markdown

```markdown
[Huawei-aaa] local-user <user-name> password cipher <password>
```

> The username may include a domain if it contains an "@" symbol. Otherwise, it uses the default domain.

1.2.1.5 Step 5: Configure User Access Type

```
[Huawei-aaa] local-user <user-name> service-type <type> <access>
```

- `<type>`:
  - terminal
  - telnet
  - ftp
  - ssh
  - snmp
  - http
- `<access>`:
  - ppp
  - none

> Set the service type for which the user is authorized. By default, all access types are disabled.

1.2.1.6 Step 6: Configure User Level

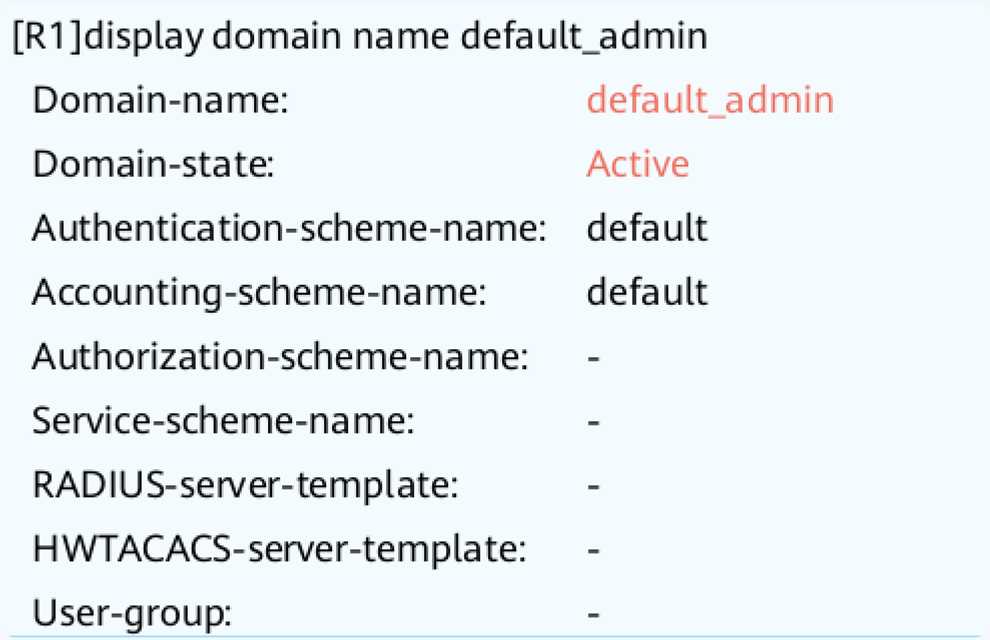
```
[Huawei-aaa] local-user <user-name> privilege level <level>
```

> Define the user's privilege level within the system.

1.2.2 Verification Commands

1.2.2.1 Display Domain Information

```
[R1]display domain name <domain-name>
```

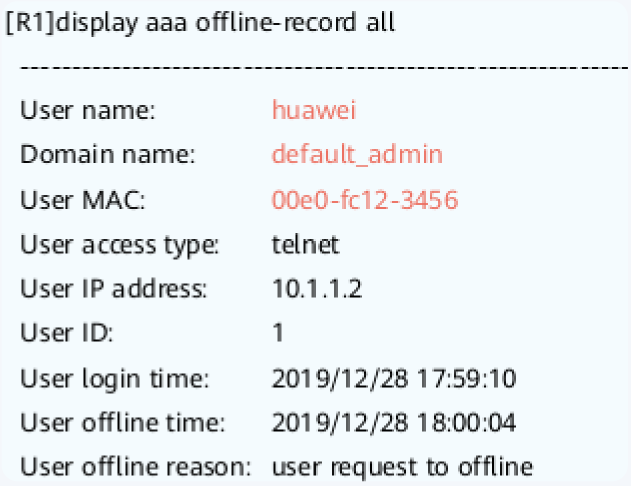


```
[R1]display domain name default_admin
  Domain-name:                   default_admin
  Domain-state:                  Active
  Authentication-scheme-name:    default
  Accounting-scheme-name:        default
  Authorization-scheme-name:     -
  Service-scheme-name:           -
  RADIUS-server-template:        -
  HWTACACS-server-template:      -
  User-group:                    -
```

> Displays configuration of `<domain-name>` domain.

1.2.2.2 Check Offline Records

```
[R1]display aaa offline-record all
```



```
[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
```

Shows records of users who have logged off from the system