

18_{AAA}

AAA refers to authentication, authorization, and accounting. In the process that a user accesses network resources, through AAA, certain rights are authorized to the user if the user passes authentication, and the original data about the user accessing network resources is recorded.

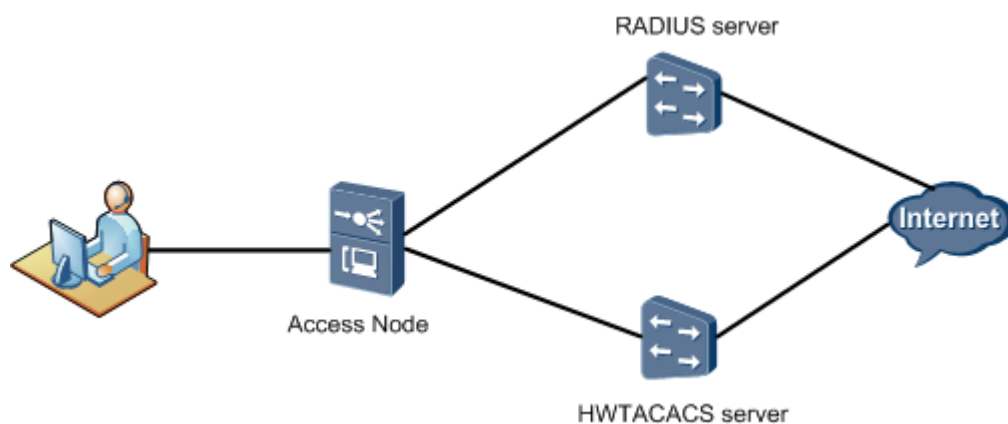
AAA includes three functions.

- Authentication: Checks whether a user is allowed to access network resources.
- Authorization: Determines what network resources a user can access.
- Accounting: Records the original data about the user accessing network resources.

AAA is generally applied to the users that access the Internet in the PPPoA, PPPoE, 802.1x, VLAN, WLAN or Admin SSH (associating the user name and the password with the domain name) mode.

In the existing network, 802.1x and Admin SSH correspond to the local AAA, that is, the access device functions as a local AAA server; PPPoE corresponds to the remote AAA, that is, the access device functions as the client of a remote AAA server.

The following picture shows an example network of the AAA application.



1. Authentication

The MA5800 supports two authentication modes: local authentication, and remote authentication.

- Local authentication: The user information (including the user name, password, and various attributes) is configured on the MA5800, and the MA5800 authenticates the user. This authentication mode is fast and can reduce carrier's cost; however, the amount of information that can be stored is limited by the device hardware.
- Remote authentication: The user information (including the user name, password, and various attributes of the user) is configured on an authentication server. The Remote Authentication Dial In User Service (RADIUS) protocol or HUAWEI Terminal Access Controller Access Control System (HWTACACS) protocol is used for remote authentication. The MA5800 serves as the authentication client and communicates with the RADIUS or HWTACACS server. When the RADIUS or HWTACACS server is faulty, the MA5800 can automatically switch to local authentication.

2. Authorization

The MA5800 supports direct authorization, local authorization, HWTACACS authorization, and if-authenticated authorization.

- Direct authorization: If trustful, a user can directly pass the authorization.
- Local authorization: A user is locally authorized according to relevant attributes of the user configured on the MA5800.
- HWTACACS authorization: The HWTACACS server authorizes a user.
- If-authenticated authorization: If a user passes the authentication and the authentication mode is not non-authentication, the user passes the authorization.

3. Accounting

The MA5800 supports non-accounting and remote accounting.

- Non-accounting: A user is not charged.
- Remote accounting: The MA5800 supports remote accounting through the AAA server.

The preceding figure shows that the AAA function can be implemented on the access device in the following three ways:

- The access device functions as a local AAA server. In this case, the local AAA needs to be configured. The local AAA does not support accounting.
- The access device functions as the client of a remote AAA server, and is connected to the RADIUS server through the RADIUS protocol, implementing the AAA. The RADIUS protocol, however, does not support authorization.
- The access device functions as the client of a remote AAA server, and is connected to the HWTACACS server through the HWTACACS protocol, implementing the AAA.

18.1 RADIUS

18.2 HWTACACS

18.3 Configuring the Local AAA

This topic describes how to configure the local AAA so that the user authentication can be performed locally.

18.4 Configuring the Remote AAA (RADIUS Protocol)

The MA5800 is interconnected with the RADIUS server through the RADIUS protocol to implement authentication and accounting.

[18.5 Configuration Example of the RADIUS Authentication and Accounting](#)

The MA5800 is interconnected with the RADIUS server through the RADIUS protocol to implement authentication and accounting.

[18.6 Configuring the Remote AAA \(HWTACACS Protocol\)](#)

The MA5800 is interconnected with the HWTACACS server through the HWTACACS protocol to implement authentication, authorization, and accounting.

[18.7 Configuration Example of the RADIUS AAA \(802.1X access user\)](#)

The MA5800 is interconnected with the RADIUS server through the RADIUS protocol to implement authentication.

[18.8 Configuration Example of HWTACACS Authentication \(Management User\)](#)

The MA5800 allows the management user of the device to log in to the system in the HWTACACS authentication mode.

18.1 RADIUS

Definition

- RADIUS is short for the remote authentication dial-in user service. It is a distributed information interaction protocol with the client-server structure. Generally, it is used to manage a large number of distributed dial-in users.
- RADIUS implements the user accounting by managing a simple user authentication database.
- The authentication and accounting requests of users can be passed on to the RADIUS server through a network access server (NAS).

Principle

- When a user tries to access another network (or some network resources) by setting up a connection to the NAS through a network, the NAS forwards the user authentication and accounting information to the RADIUS server. The RADIUS protocol specifies the means of transmitting the user information and accounting information between the NAS and the RADIUS server.
- The RADIUS server receives the connection requests of users sent from the NAS, authenticates the user account and password contained in the user authentication data, and returns the required data to the NAS.

Message Flow of the RADIUS Protocol

The RADIUS server stores the user names and passwords in a unique user authentication database for authenticating the users. When a user wishes to connect to an NE through a device and then obtain the right to access the Internet or access certain network resources, the NE authenticates the user or the corresponding connection.

The NE sends the authentication, authorization, and accounting information of the user to the RADIUS server. The RADIUS protocol specifies how the NE and the RADIUS server should exchange the user information and the accounting information. The RADIUS server receives the connection request of the user, authenticates the user, and sends the necessary configuration information of the user to the NE. The exchange of authentication information between the NE and

the RADIUS server is key protected. This protects the user password against any interception when the password is transmitted over an insecure network. [Figure 18-1](#) shows the message flow between the RADIUS client and the RADIUS server.

Figure 18-1 Message flow between the RADIUS client and the RADIUS server

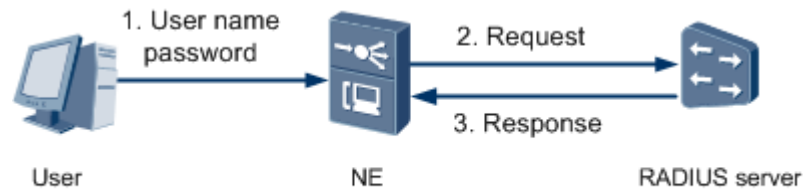
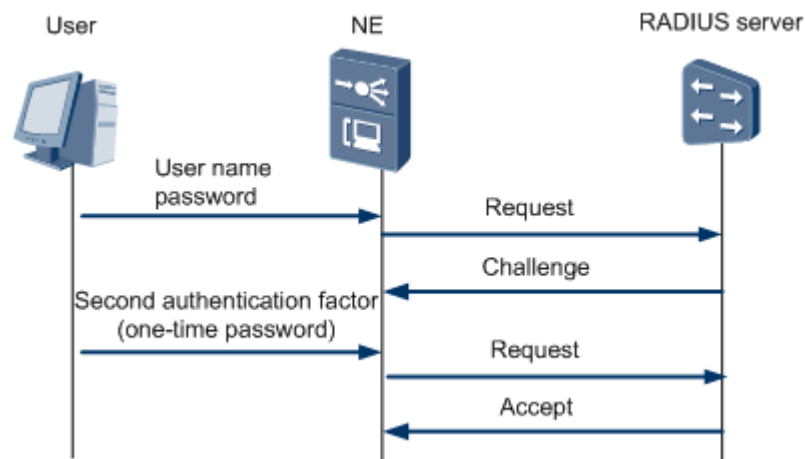


Figure 18-2 Two-factor authentication flow between the RADIUS client and the RADIUS server



NOTE

An NE refers to an access device that can function as a RADIUS client.

1. When a user logs in to the NE, the corresponding user name, password, and one-time password (required for two-factor authentication) are sent to the NE.
2. The RADIUS client on the NE receives the user name and password, and sends an authentication request to the RADIUS server.
3. The RADIUS server receives the legal request, authenticates the user, and sends the necessary authorization information of the user to the RADIUS client.

The authentication information exchanged between the RADIUS client and the RADIUS server must be encrypted before being transmitted over the network. Otherwise, the information may be intercepted when the network is insecure.

RADIUS supports the management VPN: When a carrier uses VPN to isolate management and service channels, a separated VPN can be used through RADIUS

to manage user authentication. When such a VPN is used, only the VPN used by RADIUS needs to be specified.

The accounting message flow is similar to the authentication/authorization message flow.

18.2 HWTACACS

Definition

HWTACACS (HUAWEI Terminal Access Controller Access Control System) is a security protocol enhanced based on TACACS+(draft-grant-tacacs-02). It is compatible with TACACS+ but not compatible with TACACS. Similar to the RADIUS protocol, HWTACACS implements AAA functions for multiple users by communicating with the HWTACACS server in the client/server (C/S) mode.

Purpose

HWTACACS is used for the authentication, authorization, and accounting of access users and administrators.

Principle

Adopting the client/server architecture, HWTACACS is a protocol through which the network access server (NAS) (MA5800) transmits the encrypted HWTACACS data packets to communicate with the HWTACACS database of the security server. The working mode is as follows:

- HWTACACS authentication. After being set up a connection with the NAS port, the NAS communicates with the daemon of the HWTACACS server. After the user input the user name, password, and dynamic password (if required) according to the prompt messages, the NAS sends the information to the daemon.
- HWTACACS authorization. After being authenticated, the user can be authorized. The NAS communicates with the daemon of the HWTACACS server, and then returns the accept or reject response of the authorization.

Differences Between HWTACACS and RADIUS

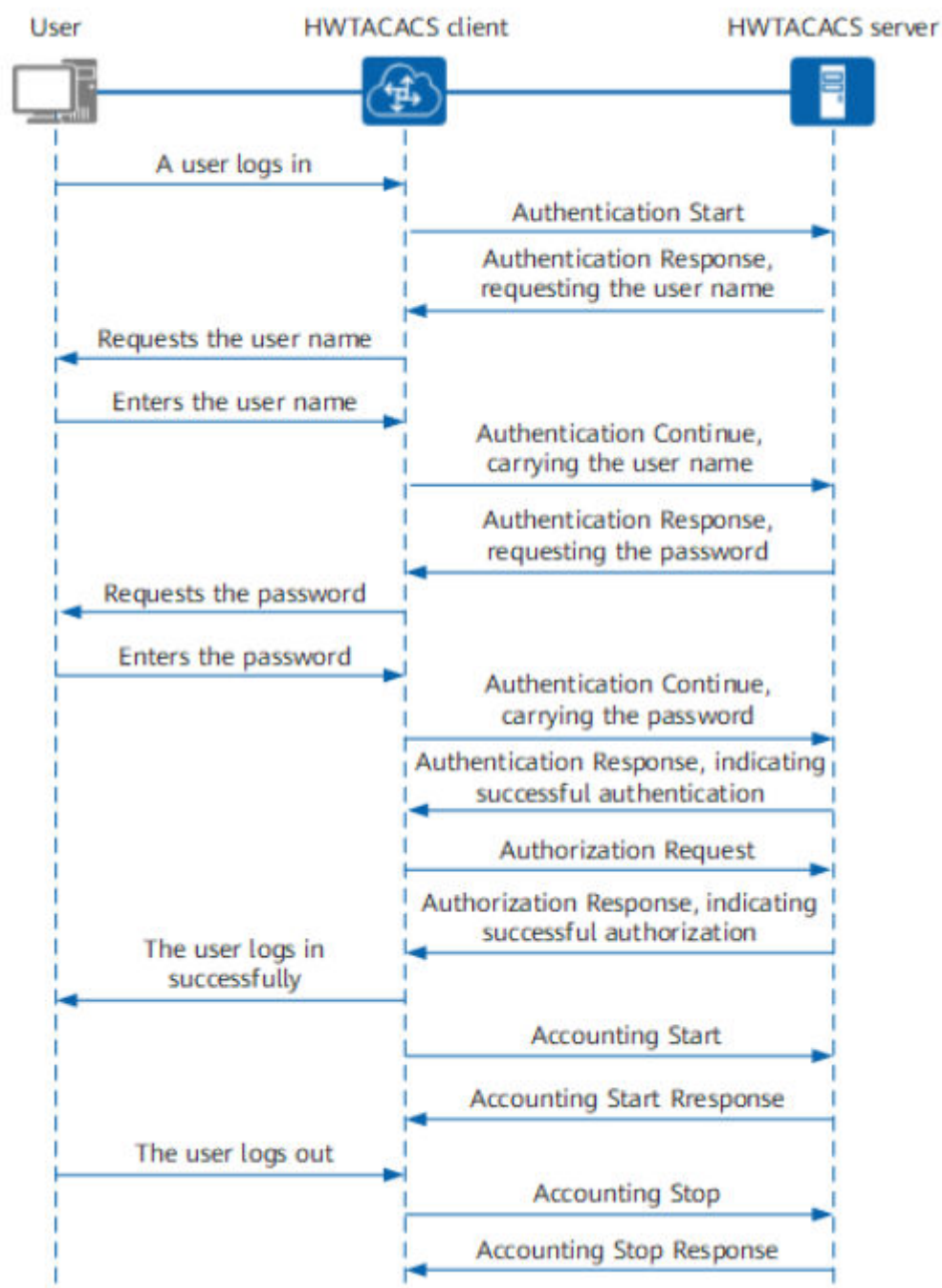
The HWTACACS message flow is similar to the RADIUS message flow. The difference is that, in the HWTACACS message flow, the server returns an authentication response rather than the user right after the user passes authentication. The user right is returned only when the authorization process is completed.

HWTACACS features more reliable transmission and encryption than RADIUS and is more suitable for security control. The following table lists the differences between HWTACACS and RADIUS.

HWTACACS	RADIUS
Uses TCP to ensure more reliable network transmission.	Uses UDP for transmission.
Encrypts the body of HWTACACS packets, except their header.	Encrypts only the password field of the authenticated packets.
Separated authorization and authentication.	Concurrent processing of authentication and authorization.
Applicable to security control.	Applicable to accounting.
Supports authorization of the configuration commands on the router.	Does not support the authorization of the configuration commands on the router.

HWTACACS Interaction Process

This section describes how HWTACACS performs authentication, authorization, and accounting for Telnet users. [Figure 18-3](#) shows the message exchange process.

Figure 18-3 HWTACACS message interaction

The following describes the HWTACACS message exchange process shown in [Figure 18-3](#):

1. A Telnet user sends a request packet.
2. After receiving the request packet, the HWTACACS client sends an Authentication Start packet to the HWTACACS server.
3. The HWTACACS server sends an Authentication Response packet to request the user name.

4. After receiving the Authentication Response packet, the HWTACACS client sends a packet to query the user name.
5. The user enters the user name.
6. The HWTACACS client sends an Authentication Continue packet containing the user name to the HWTACACS server.
7. The HWTACACS server sends an Authentication Response packet to request the password.
8. After receiving the Authentication Response packet, the HWTACACS client queries the password.
9. The user enters the password.
10. The HWTACACS client sends an Authentication Continue packet containing the password to the HWTACACS server.
11. The HWTACACS server sends an Authentication Response packet, indicating that the user has been authenticated.
12. The HWTACACS client sends an Authorization Request packet to the HWTACACS server.
13. The HWTACACS server sends an Authorization Response packet, indicating that the user has been authorized.
14. The HWTACACS client receives the Authorization Response packet and displays the login page.
15. The HWTACACS client sends an Accounting Request (start) packet to the HWTACACS server.
16. The HWTACACS server sends an Accounting Response packet.
17. The user requests to go offline.
18. The HWTACACS client sends an Accounting Request (stop) packet to the HWTACACS server.
19. The HWTACACS server sends an Accounting Response packet.

18.3 Configuring the Local AAA

This topic describes how to configure the local AAA so that the user authentication can be performed locally.

Context

- The local AAA configuration is simple, which does not depend on the external server.
- The local AAA supports authentication and authorization.

Procedure

Step 1 Configure the AAA authentication scheme.

NOTE

- The authentication scheme specifies how all the users in an Internet service provider (ISP) domain are authenticated. The system supports up to 32 authentication schemes.
- The system has a default authentication scheme named **default**. It can be modified, but cannot be deleted.

1. Run the **aaa** command to enter the AAA mode.
2. Run the **authentication-scheme** command to add an authentication scheme.
3. Run the **authentication-mode local** command to configure the authentication mode of the authentication scheme.
4. Run the **quit** command to return to the AAA mode.

Step 2 Create a domain. **NOTE**

- A domain is a group of users of the same type.
- In the user name format `userid@domain-name` (for example, `userdomain@domain.net`), "userid" indicates the user name for authentication and "domain-name" followed by "@" indicates the domain name.
- The domain name for user login cannot exceed 20 characters.
- For a user with a domain name, the total length of the user name plus @ plus the domain name cannot exceed 31 characters.

In the AAA mode, run the **domain** command to create a domain.

Step 3 Refer the authentication scheme. **NOTE**

You can use an authentication scheme in a domain only after the authentication scheme is created.

1. In the domain mode, run the **authentication-scheme** command to use the authentication scheme.
2. Run the **quit** command to return to the AAA mode.

Step 4 Create a local AAA user.

In the AAA mode, run the **local-user password** command to create a local AAA user.

Step 5 Set the access type of a local AAA user.

In the AAA mode, run the **local-user service-type** command to set the access type of a local user.

Step 6 Set the access priority of a local AAA user.

In the AAA mode, run the **local-user privilege level** command to set the access priority of a local user.

----End

Example

User 1 in the ISP domain adopts the local server for authentication. The authentication scheme is newscheme, the password is configured, and access priority is 1, do as follows:

```
huawei(config)#aaa
huawei(config-aaa)#authentication-scheme newscheme
Info: Create a new authentication scheme.
huawei(config-aaa-authen-newscheme)#authentication-mode local
huawei(config-aaa-authen-newscheme)#quit
```

```
huawei(config-aaa)#domain isp
Info: Create a new domain.
huawei(config-aaa-domain-isp)#authentication-scheme newscheme
huawei(config-aaa-domain-isp)#quit
huawei(config-aaa)#local-user user1@isp password
huawei(config-aaa)#local-user user1@isp service-type terminal
huawei(config-aaa)#local-user user1@isp privilege level 1
```

18.4 Configuring the Remote AAA (RADIUS Protocol)

The MA5800 is interconnected with the RADIUS server through the RADIUS protocol to implement authentication and accounting.

Context

- What is RADIUS:
 - RADIUS is short for the remote authentication dial-in user service. It is a distributed information interaction protocol with the client-server structure. Generally, it is used to manage a large number of distributed dial-in users.
 - RADIUS implements the user accounting by managing a simple user authentication database.
 - The authentication and accounting requests of users can be passed on to the RADIUS server through a network access server (NAS).
- Principle of RADIUS:
 - When a user tries to access another network (or some network resources) by setting up a connection to the NAS through a network, the NAS forwards the user authentication and accounting information to the RADIUS server. The RADIUS protocol specifies the means of transmitting the user information and accounting information between the NAS and the RADIUS server.
 - The RADIUS server receives the connection requests of users sent from the NAS, authenticates the user account and password contained in the user authentication data, and returns the required data to the NAS.
- Specification:
 - For the MA5800, the RADIUS is configured based on each RADIUS server group.
 - In actual networking, a RADIUS server group can be any of the following:
 - An independent RADIUS server
 - A pair of primary/secondary RADIUS servers with the same configuration but different IP addresses
 - The following lists the attributes of a RADIUS server template:
 - Primary and secondary authentication servers
 - Primary and secondary accounting servers
 - Shared key
 - Retransmission parameter

- Timeout parameter
- Whether a user name contains the domain name
- The configuration of the RADIUS protocol defines only the essential parameters for the information exchange between the MA5800 and the RADIUS server. To make the essential parameters take effect, the RADIUS server group should be referenced in a certain domain.
- The RADIUS attribute list defines the attribute parameters for interaction between the MA5800 and the RADIUS server. [Table 18-1](#) describes the parameters.

Table 18-1 RADIUS attribute list

Parameter Code	Parameter Name	Description
1	User-Name	Indicates the user name for authentication.
2	Password	Indicates the user password for authentication. This parameter is valid only for PAP authentication.
6	Service-Type	Indicates the user service type. The value of this parameter is 2 (frame) for access users and is 6 for remote management users.
7	Framed-Protocol	The value of this parameter is fixed to 7 (PPP) because ITU-T RFC2865 does not define 802.1x for this parameter.
24	State	If the access challenge packet that the RADIUS server sends to a device contains this parameter, the subsequent access request packet sent by the device to the RADIUS server must also contain this parameter of the same value as that is contained in the access challenge packet.

Parameter Code	Parameter Name	Description
25	Class	If the access accept packet sent by the RADIUS server to a device contains this parameter, the subsequent charging request packet sent by the device to the RADIUS server must also contain this parameter of the same value. For a standard RADIUS server, a device can use the Class attribute to represent the CAR parameter.
27	Session-Timeout	Indicates the available remaining time in the unit of second. It is the user re-authentication time in the EAP challenge packet.
29	Termination-Action	Indicates the service termination mode. The valid modes are re-authentication and forcing users to go offline.
32	NAS-Identifier	Indicates the host name of the device.
40	Acct-Status-Type	Indicates the charging packet type. • 1: charging start packet • 2: charging stop packet • 3: real-time charging packet
41	Acct-Delay-Time	Indicates the time for generating a charging packet in the unit of second.
44	Acct-Session-Id	Indicates the charging connection number. The connection numbers for the charging start packet, real-time charging packet, and charging stop packet of the same connection must be the same.

Parameter Code	Parameter Name	Description
45	Acct-Authentic	Indicates the user authentication mode. • 1: RADIUS authentication • 2: local authentication
46	Acct-Session-Time	Indicates the time for a user to go online in the unit of second.
49	Terminate-Cause	Indicates the user connection interruption cause. The valid values are as follows: • User-Request(1): The user actively goes offline. • Lost Carrier(2): The handshake fails, such as the EAPOL detection fails. • User Error(17): The user authentication fails or times out.
52	Acct-Input-Gigawords	Indicates the number of upstream bytes. The unit can be 4GByte, kbyte, Mbyte, or Gbyte, depending on the command configuration.
53	Acct-Output-Gigawords	Indicates the number of downstream bytes. The unit can be 4GByte, kbyte, Mbyte, or Gbyte, depending on the command configuration.
55	Event-Timestamp	Indicates the user online time in the unit of second. The value is the absolute number of seconds counting from 1970-01-01 00:00:00.
61	NAS-Port-Type	Indicates the NAS port type.
80	Message-Authenticator	Verifies validity of packets between the RADIUS server and RADIUS client to prevent malicious attacks.

Parameter Code	Parameter Name	Description
26-29 NOTE The preceding parameters are RADIUS standard attributes. Starting from this row, the following parameters are Huawei-defined attributes.	Exec-Privilege	Indicates the priority of operation users such as SSH users. The value ranges from 0 to 15. • 0: common user • 1: operator • 2-15: administrator • >15: common user
26-254	Version	Indicates the software version of the access device.
26-255	Product-ID	Indicates the product name.

Procedure

Step 1 Configure the authentication scheme.

NOTE

- The authentication scheme specifies how all the users in an ISP domain are authenticated.
- The system supports up to 32 authentication schemes. The system has a default accounting scheme named **default**. It can only be modified, but cannot be deleted.

1. Run the **aaa** command to enter the AAA mode.
2. Run the **authentication-scheme** command to add an authentication scheme.
3. Run the **authentication-mode radius** command to configure the authentication mode of the authentication scheme.
4. Run the **quit** command to return to the AAA mode.

Step 2 Configure the accounting scheme.

NOTE

- The accounting scheme specifies how all the users in an ISP domain are charged.
- The system supports up to 256 accounting schemes. The system has a default accounting scheme named **default**. It can be modified, but cannot be deleted.

1. In the AAA mode, run the **accounting-scheme** command to add an AAA accounting scheme.
2. Run the **accounting-mode radius** command to configure the accounting mode.
3. Run the **quit** command to return to the AAA mode.
4. Run the **quit** command to return to the global config mode.

Step 3 Configure the RADIUS server template.

1. Run the **radius-server template** command to create an RADIUS server template and enter the RADIUS server template mode.

2. Run the **radius-server authentication** command to configure the IP address and the UDP port ID of the RADIUS server for authentication.

 NOTE

- To guarantee normal communication between the MA5800 and the RADIUS server, before configuring the IP address and UDP port of the RADIUS server, make sure that the route between the RADIUS server and the MA5800 is in the normal state.
 - Make sure that the configuration of the RADIUS service port of the MA5800 is consistent with the port configuration of the RADIUS server.
3. Run the **radius-server accounting** command to configure the IP address and the UDP port ID of the RADIUS server for accounting.
 4. (Optional) Run the **radius-server shared-key** command to configure the shared key of the RADIUS server.

 NOTE

- The RADIUS client (MA5800) and the RADIUS server use the MD5 algorithm to encrypt the RADIUS packets. They check the validity of the packets by setting the encryption key. They can receive the packets from each other and can respond to each other only when their keys are the same.
 - You are advised to periodically update keys to ensure key security.
5. (Optional) Run the **radius-server timeout** command to set the response timeout time of the RADIUS server. By default, the timeout time is 5s.

The MA5800 sends the request packets to the RADIUS server. If the RADIUS server does not respond within the response timeout time, it re-transmits the request packets to the RADIUS to ensure that users can get corresponding services from the RADIUS server.

6. (Optional) Run the **radius-server retransmit** command to set the maximum re-transmit time of the RADIUS request packets. By default, the maximum re-transmit time is 3.

When the re-transmit time of the RADIUS request packets from the MA5800 to a RADIUS server exceeds the maximum re-transmit time, the MA5800 considers that its communication with the RADIUS server is interrupted (optional), and therefore transmits the RADIUS request packets to another RADIUS server.

7. (Optional) Run the **(undo)radius-server user-name domain-included** command to configure the user name (not) to carry the domain name when transmitted to the RADIUS server. By default, the user name of the RADIUS server carries the domain name.
 - An access user is named in the format of **userid@domain-name**, and the part after @ is the domain name. The MA5800 classifies a user into a domain according to the domain name.
 - If an RADIUS server group rejects the user name carrying the domain name, the RADIUS server group cannot be set or used in two or more domains. Otherwise, when some access users in different domains have the same user name, the RADIUS server considers that these users are the same because the names transmitted to the server are the same.
8. Run the **quit** command to return to the global config mode.

Step 4 Create a domain.

 NOTE

- A domain is a group of users of the same type.
- In the user name format `userid@domain-name` (for example, `userdomain@domain.net`), "userid" indicates the user name for authentication and "domain-name" followed by "@" indicates the domain name.
- The domain name for user login cannot exceed 20 characters.
- For a user with a domain name, the total length of the user name plus @ plus the domain name cannot exceed 31 characters.

1. Run the **aaa** command to enter the AAA mode.
2. In the AAA mode, run the **domain** command to create a domain.

Step 5 Use the authentication scheme.

You can use an authentication scheme in a domain only after the authentication scheme is created.

In the domain mode, run the **authentication-scheme** command to use the authentication scheme.

Step 6 Use the accounting scheme.

You can use an accounting scheme in a domain only after the accounting scheme is created.

In the domain mode, run the **accounting-scheme** command to use the accounting scheme.

Step 7 Use the RADIUS server template.

 NOTE

You can use a RADIUS server template in a domain only after the RADIUS server template is created.

1. In the domain mode, run the **radius-server** command to use the RADIUS server template.
2. Run the **quit** command to return to the AAA mode.

Step 8 Run the terminal **user authentication-mode AAA** command to configure automatically add a domain name to the user name for authentication when a management user logs in.

----End

Example

User 1 in the ISP domain adopts the HWTACACS protocol for authentication and accounting. The RADIUS server with the IP address 10.10.66.66 functions as the primary server for authentication and accounting. The server with the IP address 10.10.66.67 functions as the secondary server for authentication and accounting. The authentication port number is 1812, the accounting port number is 1813, and set the shared key. Other parameters adopt the default settings.

```
huawei(config)#aaa
huawei(config-aaa)#authentication-scheme newscheme
huawei(config-aaa-authen-newscheme)#authentication-mode radius
```

```
huawei(config-aaa-authen-newscheme)#quit
huawei(config-aaa)#accounting-scheme newscheme
huawei(config-aaa-accounting-newscheme)#accounting-mode radius
huawei(config-aaa-accounting-newscheme)#quit
huawei(config-aaa)#quit
huawei(config)#radius-server template hwtest
huawei(config-radius-hwtest)#radius-server shared-key
huawei(config-radius-hwtest)#radius-server authentication 10.10.66.66 1812
huawei(config-radius-hwtest)#radius-server authentication 10.10.66.67 1812 secondary
huawei(config-radius-hwtest)#radius-server accounting 10.10.66.66 1813
huawei(config-radius-hwtest)#radius-server accounting 10.10.66.67 1813 secondary
huawei(config-radius-hwtest)#quit
huawei(config)#aaa
huawei(config-aaa)#domain isp
huawei(config-aaa-domain-isp)#authentication-scheme newscheme
huawei(config-aaa-domain-isp)#accounting-scheme newscheme
huawei(config-aaa-domain-isp)#radius-server hwtest
huawei(config-aaa-domain-isp)#quit
huawei(config-aaa)#quit
huawei(config)#terminal user authentication-mode AAA isp
```

18.5 Configuration Example of the RADIUS Authentication and Accounting

The MA5800 is interconnected with the RADIUS server through the RADIUS protocol to implement authentication and accounting.

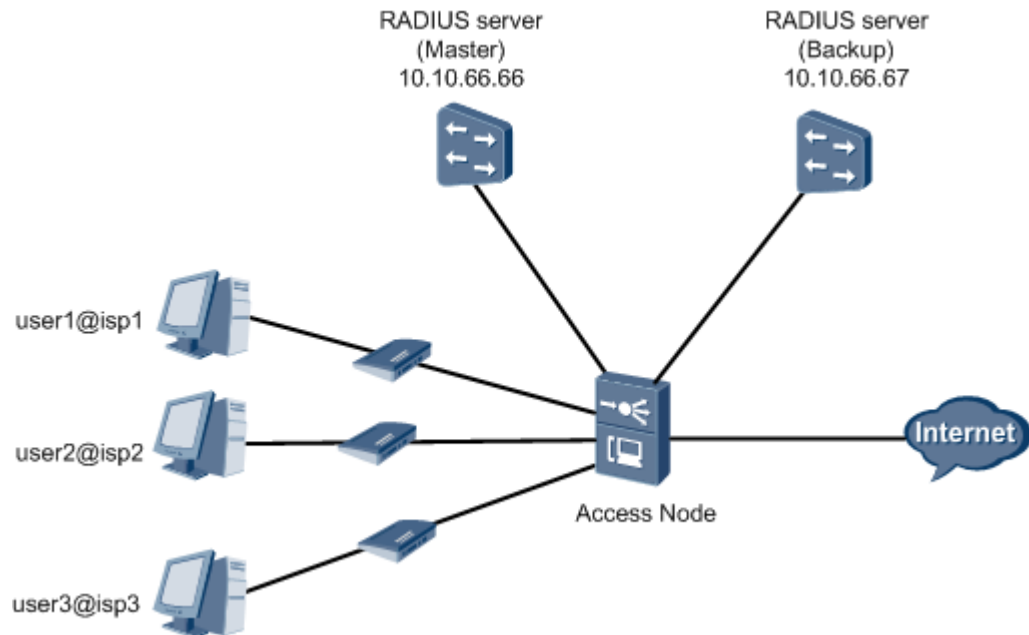
Service Requirements

- The RADIUS server performs authentication and accounting for User 1 in the isp1 domain.
- The RADIUS server with the IP address 10.10.66.66 functions as the primary server for authentication and accounting.
- The RADIUS server with the IP address 10.10.66.67 functions as the secondary server for authentication and accounting.
- The authentication port number is 1812, and the accounting port number is 1813.
- Set shared key of the RADIUS server.
- Other parameters adopt the default settings.

Networking

Figure 18-4 shows an example network of the RADIUS Authentication and Accounting application.

Figure 18-4 Example network of the RADIUS Authentication and Accounting application.



Procedure

Step 1 Configure the authentication scheme.

Configure authentication scheme named **newscheme** (users are authenticated through RADIUS).

```
huawei(config)#aaa
huawei(config-aaa)#authentication-scheme newscheme
huawei(config-aaa-authen-newscheme)#authentication-mode radius
huawei(config-aaa-authen-newscheme)#quit
```

Step 2 Configure the accounting scheme.

Configure accounting scheme named **newscheme** (users are accounted through RADIUS).

```
huawei(config-aaa)#accounting-scheme newscheme
huawei(config-aaa-accounting-newscheme)#accounting-mode radius
huawei(config-aaa-accounting-newscheme)#quit
huawei(config-aaa)#quit
```

Step 3 Configure the RADIUS protocol.

Create RADIUS server template named **hwtest** with the RADIUS server 10.10.66.66 as the primary authentication and accounting server, the RADIUS server 10.10.66.67 as the secondary authentication and accounting server, and set the shared key.

```
huawei(config)#radius-server template hwtest
Info: A new server-template is created.
Warning: Please configure the shared-key. Configuring shared-key is mandatory
to communicate with RADIUS server.
huawei(config-radius-hwtest)#radius-server shared-key
huawei(config-radius-hwtest)#radius-server authentication 10.10.66.66 1812
```

```
huawei(config-radius-hwtest)#radius-server authentication 10.10.66.67 1812 secondary
huawei(config-radius-hwtest)#radius-server accounting 10.10.66.66 1813
huawei(config-radius-hwtest)#radius-server accounting 10.10.66.67 1813 secondary
huawei(config-radius-hwtest)#quit
```

Step 4 Create a domain.

Create a domain named isp1.

```
huawei(config)#aaa
huawei(config-aaa)#domain isp1
Info: Create a new domain.
```

Step 5 Use the authentication scheme.

You can use an authentication scheme in a domain only after the authentication scheme is created.

```
huawei(config-aaa-domain-isp1)#authentication-scheme newscheme
```

Step 6 Use the accounting scheme.

You can use an accounting scheme in a domain only after the accounting scheme is created.

```
huawei(config-aaa-domain-isp1)#accounting-scheme newscheme
```

Step 7 Use the RADIUS server template.

You can use a RADIUS server template in a domain only after the RADIUS server template is created.

```
huawei(config-aaa-domain-isp1)#radius-server hwtest
huawei(config-aaa-domain-isp1)#quit
```

----End

Result

User 1 in isp1 can pass authentication only if both the user name and password are correct, and then can log in to the MA5800. Then, the user starts to be accounted.

Configuration File

```
aaa
authentication-scheme newscheme
authentication-mode radius
quit
accounting-scheme newscheme
accounting-mode radius
quit
quit
radius-server template hwtest
radius-server shared-key
radius-server authentication 10.10.66.66 1812
radius-server authentication 10.10.66.67 1812 secondary
radius-server accounting 10.10.66.66 1813
radius-server accounting 10.10.66.67 1813 secondary
quit
aaa domain isp1 authentication-scheme newscheme
accounting-scheme newscheme
radius-server hwtest
quit
```

18.6 Configuring the Remote AAA (HWTACACS Protocol)

The MA5800 is interconnected with the HWTACACS server through the HWTACACS protocol to implement authentication, authorization, and accounting.

Context

- What is HWTACACS:
 - HWTACACS is a security protocol with enhanced functions on the base of TACACS+(draft-grant-tacacs-02). Similar to the RADIUS protocol, HWTACACS implements multiple subscriber AAA functions through communications with the HWTACACS server in the client/server (C/S) mode.
 - HWTACACS is used for the authentication, authorization, and accounting for the management users.
- Principle of HWTACACS:

Adopting the client/server architecture, HWTACACS is a protocol through which the NAS (MA5800) transmits the encrypted HWTACACS data packets to communicate with the HWTACACS database of the security server. The working mode is as follows:

 - HWTACACS authentication. When the remote user connects to the corresponding port of the NAS, the NAS communicates with the daemon of the HWTACACS server, and obtains the prompt of entering the user name from the daemon. Then, the NAS displays the message to the user. When the remote user enters the user name, the NAS transmits the user name to the daemon. Then, the NAS obtains the prompt of entering the password, and displays the message to the user. After the remote user enters the password, the NAS transmits the password to the daemon.
 - HWTACACS authorization. After being authenticated, the user can be authorized. The NAS communicates with the daemon of the HWTACACS server, and then returns the accept or reject response of the authorization.

NOTE

- The HWTACACS configuration only defines the parameters used for data exchange between the MA5800 and the HWTACACS server. To make these parameters take effect, you need to use the HWTACACS server group in a domain.
- The settings of an HWTACACS server template can be modified regardless of whether the template is bound to a server or not.

Procedure

Step 1 Configure the AAA authentication scheme.

The authentication scheme specifies how all the users in an ISP domain are authenticated.

The system supports up to 32 authentication schemes. The system has a default authentication scheme named **default**. It can be modified, but cannot be deleted.

1. Run the **aaa** command to enter the AAA mode.
2. Run the **authentication-scheme** command to add an authentication scheme.
3. Run the **authentication-mode hwtacacs** command to configure the authentication mode of the authentication scheme. Use the HWTACACS protocol to authenticate users.
4. Run the **quit** command to return to the AAA mode.

Step 2 Configure the AAA authorization scheme.

The authorization scheme specifies how all the users in an ISP domain are authorized.

1. In the AAA mode, run the **authorization-scheme** command to add an AAA authorization scheme.
2. Run the **authorization-mode hwtacacs** command to configure the authorization mode.
3. Run the **quit** command to return to the AAA mode.

Step 3 Configure the AAA accounting scheme.

The accounting scheme specifies how all the users in an ISP domain are charged.

The system supports up to 256 accounting schemes. The system has a default accounting scheme named **default**. It can be modified, but cannot be deleted.

1. In the AAA mode, run the **accounting-scheme** command to add an AAA accounting scheme.
2. Run the **accounting-mode hwtacacs** command to configure the accounting mode. By default, the accounting is not performed.
3. Run the **quit** command to return to the AAA mode.
4. Run the **quit** command to return to the global config mode.

Step 4 Configure the HWTACACS protocol.

The configuration of the HWTACACS protocol of the MA5800 is on the basis of the HWTACACS server group. In actual networking scenarios, an HWTACACS server group can be an independent HWTACACS server or a combination of two HWTACACS servers, that is, a primary server and a secondary server with the same configuration but different IP addresses.

Each HWTACACS server template contains the primary/secondary server IP address, shared key, and HWTACACS server type.

Primary and secondary authentication, accounting, and authorization servers can be configured. The IP address of the primary server, however, must be different from that of the secondary server. Otherwise, the configuration of primary and secondary servers will fail. By default, the IP addresses of the primary and secondary servers are both 0.0.0.0.

1. Run the **hwtacacs-server template** command to create an HWTACACS server template and enter the HWTACACS server template mode.
2. Run the **hwtacacs-server authentication** command to configure a primary authentication server. You can select **secondary** to configure a secondary authentication server.

 NOTE

- To ensure normal communication between the MA5800 and the HWTACACS server, before configuring the IP address and the TCP port of the HWTACACS server, make sure that the route between the HWTACACS server and the MA5800 is in the normal state.
 - Make sure that the HWTACACS server port of the MA5800 is the same as the port of the HWTACACS server.
3. Run the **hwtacacs-server accounting** command to configure a primary accounting server. You can select **secondary** to configure a secondary accounting server.
 4. Run the **hwtacacs-server authorization** command to configure a primary authorization server. You can select **secondary** to configure a secondary authorization server.
 5. (Optional) Run the **hwtacacs-server shared-key** command to configure the shared key of the HWTACACS server.

 NOTE

- The HWTACACS client (MA5800) and the HWTACACS server use the MD5 algorithm to encrypt the HWTACACS packets. They check the validity of the packets by configuring the encryption key. They can receive the packets from each other and can respond to each other only when their keys are the same.
 - By default, the HWTACACS server does not have a key. You are advised to configure and periodically update keys to ensure key security.
6. (Optional) Run the **hwtacacs-server timer response-timeout** to set the response timeout time of the HWTACACS server.

 NOTE

- If the HWTACACS server does not respond to the HWTACACS request packets within the timeout time, the communication with the current HWTACACS server is considered as interrupted.
 - By default, the response timeout time of the HWTACACS server is 5s.
7. (Optional) In the global config mode, run the **hwtacacs-server accounting-stop-packet** command to configure the re-transmission mechanism of the accounting-stop packets of the HWTACACS server.

 NOTE

- To prevent the loss of the accounting packets, the MA5800 supports the re-transmission of the accounting-stop packets of the HWTACACS server.
 - By default, the re-transmit time of the accounting-stop packets of the HWTACACS server is 100.
8. (Optional) Run the **(undo) hwtacacs-server user-name domain-included** command to configure the user name (not) to carry the domain name when transmitted to the HWTACACS server.
 - By default, the user name of the HWTACACS server carries the domain name.
 - After the **undo hwtacacs-server user-name domain-included** command is executed, the domain name is deleted from the user name when the client sends authentication and authorization requests to the HWTACACS server. The domain name in the user name of the accounting request is, however, reserved. This is to ensure that the users can be distinguished from each other in the accounting.

9. Run the **quit** command to return to the global config mode.

Step 5 Create a domain.

 NOTE

- A domain is a group of users of the same type.
- In the user name format `userid@domain-name` (for example, `userdomain@domain.net`), "userid" indicates the user name for authentication and "domain-name" followed by "@" indicates the domain name.
- The domain name for user login cannot exceed 20 characters.
- For a user with a domain name, the total length of the user name plus @ plus the domain name cannot exceed 31 characters.

1. Run the **aaa** command to enter the AAA mode.
2. In the AAA mode, run the **domain** command to create a domain.

Step 6 Use the authentication scheme.

You can use an authentication scheme in a domain only after the authentication scheme is created.

In the domain mode, run the **authentication-scheme** command to use the authentication scheme.

Step 7 Use the accounting scheme.

You can use an accounting scheme in a domain only after the accounting scheme is created.

In the domain mode, run the **accounting-scheme** command to use the accounting scheme.

Step 8 Use the authorization scheme.

You can use an authorization scheme in a domain only after the authorization scheme is created.

In the domain mode, run the **authorization-scheme** command to use the authorization scheme.

Step 9 Use the HWTACACS server template.

You can use an HWTACACS server template in a domain only after the HWTACACS server template is created.

1. In the domain mode, run the **hwtacacs-server** command to use the HWTACACS server template.
2. Run the **quit** command to return to the AAA mode.

Step 10 Run the terminal **user authentication-mode AAA** command to configure automatically add a domain name to the user name for authentication when a management user logs in.

----End

Example

User 1 in the ISP domain adopts the HWTACACS protocol for authentication, authorization, and accounting. HWTACACS server 10.10.66.66 functions as the

primary authentication, authorization, and accounting server, and HWTACACS server 10.10.66.67 functions as the standby authentication, authorization, and accounting server. On the HWTACACS server, set the shared key, the parameters adopt the default values. To perform the preceding configuration, do as follows:

```
huawei(config)#aaa
huawei(config-aaa)#authentication-scheme newscheme
huawei(config-aaa-authen-newscheme)#authentication-mode hwtacacs
huawei(config-aaa-authen-newscheme)#quit
huawei(config-aaa)#authorization-scheme newscheme
huawei(config-aaa-author-newscheme)#authorization-mode hwtacacs
huawei(config-aaa-author-newscheme)#quit
huawei(config-aaa)#accounting-scheme newscheme
huawei(config-aaa-accounting-newscheme)#accounting-mode hwtacacs
huawei(config-aaa-accounting-newscheme)#quit
huawei(config-aaa)#quit
huawei(config)#hwtacacs-server template hwtest
huawei(config-hwtacacs-hwtest)#hwtacacs-server shared-key
huawei(config-hwtacacs-hwtest)#hwtacacs-server authentication 10.10.66.66
huawei(config-hwtacacs-hwtest)#hwtacacs-server authentication 10.10.66.67 secondary
huawei(config-hwtacacs-hwtest)#hwtacacs-server authorization 10.10.66.66
huawei(config-hwtacacs-hwtest)#hwtacacs-server authorization 10.10.66.67 secondary
huawei(config-hwtacacs-hwtest)#hwtacacs-server accounting 10.10.66.66
huawei(config-hwtacacs-hwtest)#hwtacacs-server accounting 10.10.66.67 secondary
huawei(config-hwtacacs-hwtest)#quit
huawei(config)#aaa
huawei(config-aaa)#domain isp
huawei(config-aaa-domain-isp)#authentication-scheme newscheme
huawei(config-aaa-domain-isp)#authorization-scheme newscheme
huawei(config-aaa-domain-isp)#accounting-scheme newscheme
huawei(config-aaa-domain-isp)#hwtacacs-server hwtest
huawei(config-aaa-domain-isp)#quit
huawei(config-aaa)#quit
huawei(config)#terminal user authentication-mode AAA isp
```

18.7 Configuration Example of the RADIUS AAA (802.1X access user)

The MA5800 is interconnected with the RADIUS server through the RADIUS protocol to implement authentication.

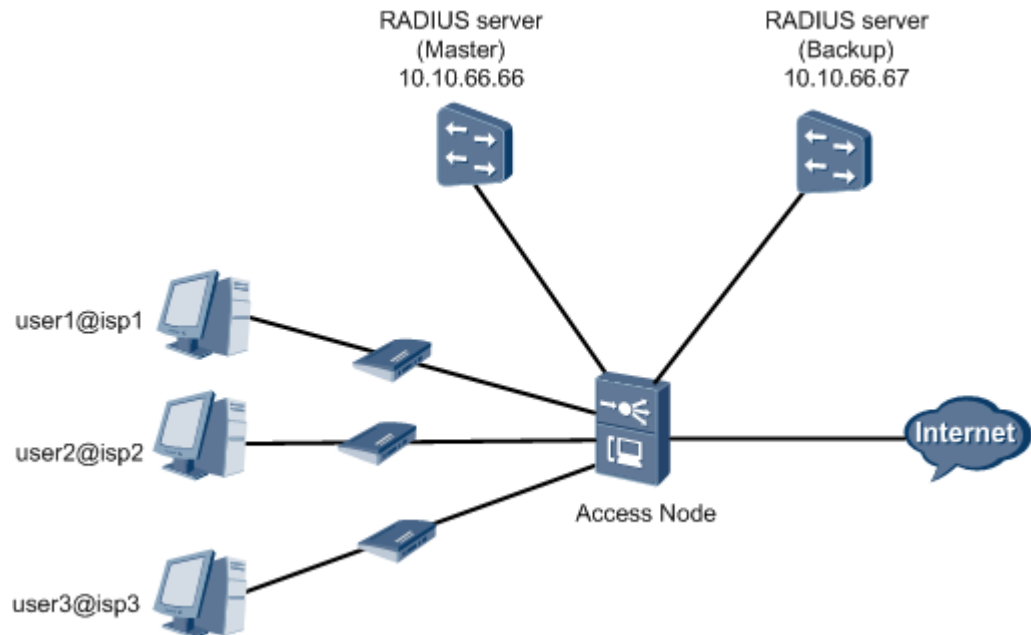
Service Requirements

- The RADIUS server performs authentication for 802.1X access users of isp1.
- The user logs in to the server carrying the domain name.
- The RADIUS server with the IP address 10.10.66.66 functions as the primary server for authentication.
- The RADIUS server with the IP address 10.10.66.67 functions as the secondary server for authentication.
- Other parameters adopt the default settings.

Networking

[Figure 18-5](#) shows an example network of the RADIUS authentication.

Figure 18-5 Example network of the RADIUS Authentication and Accounting application.



Procedure

Step 1 Configure the authentication scheme.

Configure the authentication scheme named **newscheme** (users are authenticated through RADIUS).

```

huawei(config)#aaa
huawei(config-aaa)#authentication-scheme newscheme
huawei(config-aaa-authen-newscheme)#authentication-mode radius
huawei(config-aaa-authen-newscheme)#quit
huawei(config-aaa)#quit
  
```

Step 2 Configure the RADIUS protocol.

Create RADIUS server template named **hwtest** with the RADIUS server 10.10.66.66 as the primary authentication server, and the RADIUS server 10.10.66.67 as the secondary authentication server.

NOTE

Run the **(undo) radius-server user-name domain-included** command to configure the user name (not) to carry the domain name when transmitted to the RADIUS server.

- By default, the user name of the RADIUS server carries the domain name.
- After the **undo radius-server user-name domain-included** command is executed, the domain name is deleted from the user name when a client sends an authentication request to the RADIUS server.

```

huawei(config)#radius-server template hwtest
Info: A new server-template is created.
Warning: Please configure the shared-key. Configuring shared-key is mandatory to communicate with RADIUS server.
huawei(config-radius-hwtest)#radius-server shared-key
huawei(config-radius-hwtest)#radius-server authentication 10.10.66.66 1812
  
```

```
huawei(config-radius-hwtest)#radius-server authentication 10.10.66.67 1812 secondary
huawei(config-radius-hwtest)#quit
```

Step 3 Configure the 802.1X authentication.

1. Enable the 802.1X global switch. Enable the 802.1X authentication for ports 1. The 802.1X needs to be triggered by DHCP. Therefore, the DHCP-trigger authentication must be enabled.

```
huawei(config)#dot1x enable
huawei(config)#dot1x service-port 1
huawei(config)#dot1x dhcp-trigger enable
huawei(config)#dhcp option82 enable
```

2. Configure an 802.1X parameters. In the local termination authentication, the 802.1X parameters should be configured to be in the EAP termination mode. The count of allowed handshake failure is 1 and the handshake interval is 20s.

```
huawei(config)#dot1x keepalive retransmit 1 interval 20 service-port 1
huawei(config)#dot1x eap-end service-port 1
```

Step 4 Create a domain. **NOTE**

- A domain is a group of users of the same type.
- In the user name format userid@domain-name (for example, userdomain@domain.net), "userid" indicates the user name for authentication and "domain-name" followed by "@" indicates the domain name.
- The domain name for user login cannot exceed 20 characters.
- For a user with a domain name, the total length of the user name plus @ plus the domain name cannot exceed 31 characters.

Create a domain named isp1.

```
huawei(config)#aaa
huawei(config-aaa)#domain isp1
Info: Create a new domain
```

Step 5 Use the authentication scheme.

You can use an authentication scheme in a domain only after the authentication scheme is created.

```
huawei(config-aaa-domain-isp1)#authentication-scheme newscheme
```

Step 6 Bind the RADIUS server template.

You can use a RADIUS server template in a domain only after the RADIUS server template is created.

```
huawei(config-aaa-domain-isp1)#radius-server hwtest
```

----End

Result

User 1 in isp1 can pass authentication only if both the user name and password are correct, and then can log in to the MA5800.

Configuration File

```
aaa
authentication-scheme newscheme
authentication-mode radius
```

```
quit
quit

radius-server template hwtest
radius-server shared-key
radius-server authentication 10.10.66.66 1812
radius-server authentication 10.10.66.67 1812 secondary
quit
dot1x enable
dot1x service-port 1
dot1x dhcp-trigger enable
dhcp option82 enable
dot1x keepalive retransmit 1 interval 20 service-port 1
dot1x eap-end service-port 1

domain isp1
authentication-scheme newscheme
radius-server hwtest
```

18.8 Configuration Example of HWTACACS Authentication (Management User)

The MA5800 allows the management user of the device to log in to the system in the HWTACACS authentication mode.

Prerequisites

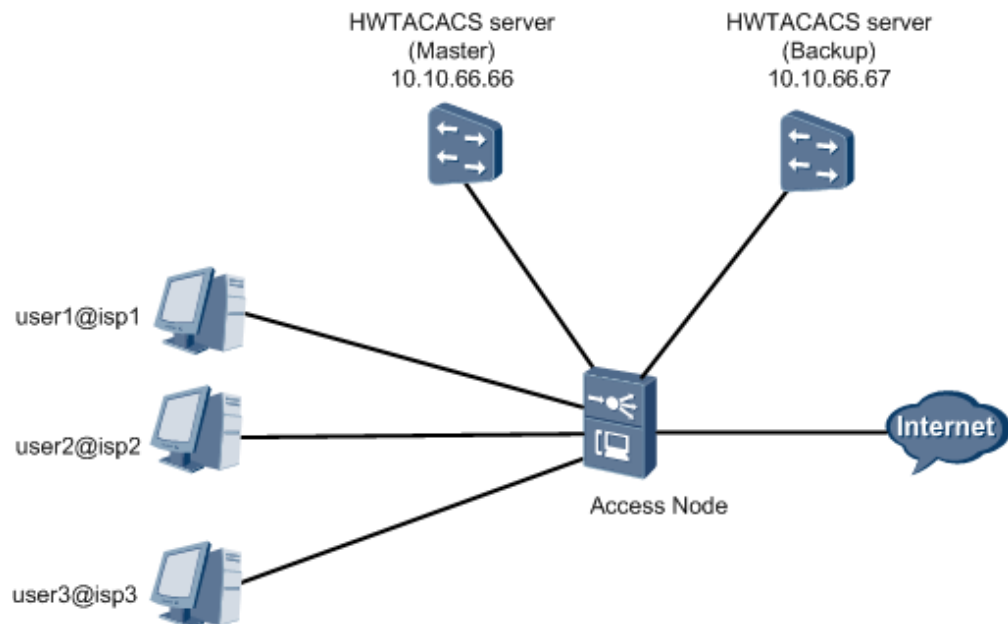
- The route from the MA5800 to the HWTACACS server must be configured.
- The management user information (user name@domain and password) must be configured on the HWTACACS server.

Service Requirements

- The HWTACACS server performs authentication for management user of domain **isp1**.
- The user logs in to the server carrying the domain name.
- The HWTACACS server with the IP address 10.10.66.66 functions as the primary server for authentication.
- The HWTACACS server with the IP address 10.10.66.67 functions as the secondary server for authentication.
- Other parameters adopt the default settings.

Networking

[Figure 18-6](#) shows an example network of HWTACACS authentication.

Figure 18-6 Example network of HWTACACS authentication

Procedure

Step 1 Configure the authentication scheme.

Configure authentication scheme named **login-auth** (users are authenticated and authorized through HWTACACS).

```
huawei(config)#aaa
huawei(config-aaa)#authentication-scheme login-auth
huawei(config-aaa-authen-login-auth)#authentication-mode hwtacacs
huawei(config-aaa-authen-login-auth)#quit
huawei(config-aaa)#authorization-scheme login-auth
huawei(config-aaa-author-login-auth)#authorization-mode hwtacacs
huawei(config-aaa-author-login-auth)#quit
huawei(config-aaa)#quit
```

Step 2 Configure the HWTACACS protocol.

Create the HWTACACS server template named **hw-login** with HWTACACS server 10.10.66.66 as the primary authentication server, and HWTACACS server 10.10.66.67 as the secondary authentication server. Set the shared key.

```
huawei(config)#hwtacacs-server template hw-login
Info: Create a new HWTACACS-server template.
Warning: To improve the service security, please run the hwtacacs-server
shared-key command to configure a shared key.
huawei(config-hwtacacs-hw-login)#hwtacacs-server shared-key
huawei(config-hwtacacs-hw-login)#hwtacacs-server authentication 10.10.66.66 1812
huawei(config-hwtacacs-hw-login)#hwtacacs-server authentication 10.10.66.67 1812 secondary
huawei(config-hwtacacs-hw-login)#hwtacacs-server authorization 10.10.66.66 1812
huawei(config-hwtacacs-hw-login)#hwtacacs-server authorization 10.10.66.67 1812 secondary
huawei(config-hwtacacs-hw-login)#quit
```

Step 3 Create a domain named isp1.

 NOTE

- A domain is a group of users of the same type.
- In the user name format `userid@domain-name` (for example, `userdomain@domain.net`), "userid" indicates the user name for authentication and "domain-name" followed by "@" indicates the domain name.
- The domain name for user login cannot exceed 20 characters.
- For a user with a domain name, the total length of the user name plus @ plus the domain name cannot exceed 31 characters.

```
huawei(config)#aaa
huawei(config-aaa)#domain isp1
Info: Create a new domain.
```

Step 4 Use the authentication scheme **login-auth**.

You can use an authentication scheme in a domain only after the authentication scheme is created.

```
huawei(config-aaa-domain-isp1)#authentication-scheme login-auth
huawei(config-aaa-domain-isp1)#authorization-scheme login-auth
```

Step 5 Bind the HWTACACS server template **hw-login** to the user.

You can use an HWTACACS server template in a domain only after the HWTACACS server template is created.

```
huawei(config-aaa-domain-isp1)#hwtacacs-server hw-login
huawei(config-aaa-domain-isp1)#quit
huawei(config-aaa)#quit
```

----End

Result

- When the HWTACACS server is reachable, the management user can log in to the MA5800 through SSH. After entering the user name and password specified on the HWTACACS server, the management user can successfully log in to the MA5800.
- When the HWTACACS server is unreachable, a user cannot log in to the MA5800 in SSH mode by entering the user name and password specified on the HWTACACS server.

Configuration File

```
aaa
authentication-scheme login-auth
authentication-mode hwtacacs
quit
authorization-scheme login-auth
authorization-mode hwtacacs
quit
quit

hwtacacs-server template hw-login
hwtacacs-server shared-key
hwtacacs-server authentication 10.10.66.66
hwtacacs-server authentication 10.10.66.67 secondary
hwtacacs-server authorization 10.10.66.66
hwtacacs-server authorization 10.10.66.67 secondary
quit
aaa
```

```
domain isp1
authentication-scheme login-auth
authorization-scheme login-auth
hwtacacs-server hw-login
quit
quit
```