Table of Contents

Chapter 1 New AAA&Radius Features 1-1
1.1 AAA Separation 1-1
1.1.1 Configuring Separate AAA Schemes 1-1
1.1.2 Configuration Example for Separate AAA Schemes 1-2
1.2 User Re-authentication at Reboot 1-4
1.2.1 Configuring User Re-authentication at Reboot 1-5
1.2.2 Configuration Example for User Re-authentication at Reboot 1-5
1.3 Tag VLAN Assignment on Trunk/Hybrid Port Supported by 802.1x Authentication 1-5
1.4 Identifier Authentication Method Attribute in RADIUS 1-6
1.5 Dynamic VLAN Assignment 1-6
1.5.1 Configuring Dynamic VLAN Assignment 1-6
1.5.2 Configuration Example for Dynamic VLAN Assignment 1-7
Chapter 2 New AAA&Radius Features Commands 2-1
2.1 New AAA&Radius Features Commands 2-1
2.1.1 accounting 2-1
2.1.2 accounting-on enable 2-2
2.1.3 authentication 2-3
2.1.4 authorization 2-5
2.1.5 name 2-5
2.1.6 vlan-assignment-mode 2-6

Chapter 1 New AAA&Radius Features

1.1 AAA Separation

AAA (authentication, authorization and accounting) is a management framework for network access control. It provides the following three services:

- Authentication: Checks if a user can access the network.
- Authorization: Authorizes a user to use a specific service.
- Accounting: Records the network usage of a user.

In AAA management, you can use the **authentication**, **authorization**, and **accounting** commands separately to specify a scheme for each of the three AAA functions (authentication, authorization and accounting) respectively. This AAA separation feature brings flexibility to AAA configuration. The following lists the implementations of AAA separation for the services supported by AAA.

- For terminal users

Authentication method: RADIUS, local, RADIUS-local, or none.

Authorization method: none.

Accounting method: RADIUS or none.

You can configure combined authentication, authorization and accounting schemes depending on the methods supported by the switch according to your needs.

- For FTP users

Only authentication is supported for FTP users.

Authentication method: RADIUS, local, or RADIUS-local.

1.1.1 Configuring Separate AAA Schemes

Table 1-1 Configure separate AAA schemes

Operation	Command	Description
Enter system view	**system-view**	—
Create an ISP domain or enter an existing ISP domain view	**domain** *isp-name*	Required
Configure an authentication scheme for the ISP domain	**authentication** { **radius-scheme** *radius-scheme-name* [**local**] | **local** | **none** }	Optional By default, no separate authentication scheme is configured.

Operation	Command	Description
Allow users in current ISP domain to use network services without being authorized	**authorization none**	Optional By default, no separate authorization scheme is configured.
Configure an accounting scheme for the ISP domain	**accounting** { **none** | **radius-scheme** *radius-scheme-name* }	Optional By default, no separate accounting scheme is configured.

Note:

- If a bound AAA scheme (that is, the authentication, authorization and accounting are bound in one scheme) is configured as well as the separate authentication, authorization and accounting schemes, the separate ones will be adopted in precedence.
- RADIUS scheme and local scheme do not support the separation of authentication and authorization. Therefore, pay attention when you perform authentication and authorization configuration: when the **scheme radius-scheme** or **scheme local** command is executed and the **authentication** command is not executed, the authorization information returned from the RADIUS or local scheme will still take effect even if the **authorization none** command is executed.

1.1.2 Configuration Example for Separate AAA Schemes

I. Network requirements

A RADIUS server with IP address 10.110.91.164 is connected to the switch. This server will be used as an authentication server.

On the switch, set the shared key it uses to exchange packets with the RADIUS server to "expert".

Configure the RADIUS scheme radius as both the authentication and accounting schemes of the ISP domain cams, and allow users in this ISP domain to use network services without being authorized.

II. Network diagram

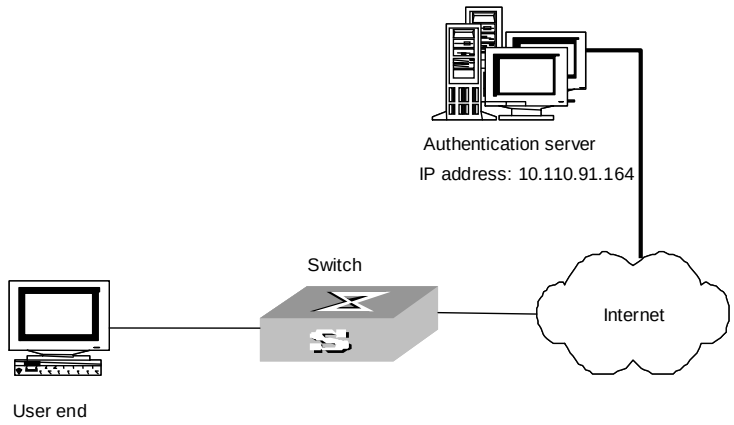

Figure 1-1 Network diagram for separate AAA schemes

III. Configuration procedure

Enter system view.

```
<Quidway> system-view
```

Create an ISP domain named cams.

```
[Quidway] domain cams
```

Return to system view.

```
[Quidway-isp-cams] quit
```

Configure a RADIUS scheme named radius.

```
[Quidway] radius scheme radius
[Quidway-radius-radius] primary accounting 10.110.91.164 1813
[Quidway-radius-radius] primary authentication 10.110.91.164 1812
[Quidway-radius-radius] key authentication expert
[Quidway-radius-radius] user-name-format with-domain
[Quidway-radius-radius] quit
```

Enter the ISP domain cams.

```
[Quidway] domain cams
```

Configure the RADIUS scheme radius as both the authentication and accounting schemes of the ISP domain cams, and allow users in this ISP domain to use network services without being authorized.

```
[Quidway-isp-cams] authentication radius-scheme radius
[Quidway-isp-cams] accounting radius-scheme radius
[Quidway-isp-cams] authorization none
```

1.2 User Re-authentication at Reboot

Note:

The feature applies to the environments where the RADIUS authentication/accounting server is CAMS.

In an AAA scheme implemented jointly by the switch and CAMS, if the switch reboots after an exclusive user (a user whose concurrent online number is set to 1 on the CAMS) passes the authentication, gets authorized and begins being charged, the switch will give a prompt that the user has already been online when the user re-logs onto the network before the CAMS makes online detection. Therefore, the user cannot access network resources as usual. In this situation, the user can log onto the network again only after the network administrator manually removes the user's online information.

The user re-authentication at reboot feature is designed to resolve this problem. After this feature is enabled, every time the switch reboots:

- The switch generates an Accounting-On packet, which mainly contains the following information: NAS-ID, NAS-IP (source IP address), and session ID.
- The switch sends the Accounting-On packet to the CAMS at regular intervals.
- Once the CAMS receives the Accounting-On packet, it sends a response to the switch. At the same time it finds and deletes the existing online information of the users who were accessing the network through the switch before the reboot based on the NAS-ID, NAS-IP and session ID contained in the Accounting-On packet, and ends the charging of the users according to the last accounting update packet.
- Once the switch receives the response from the CAMS, it stops sending other Accounting-On packets.
- If the switch has tried the set maximum times to transmit the Accounting-On packet but still does not receive any response from the CAMS, it stops the sending of the Accounting-On packet.

Note:

The switch can automatically generate the main attributes (NAS-ID, NAS-IP and session ID) of the Accounting-On packets. However, you can also manually configure the NAS-IP attribute with the **nas-ip** command. When doing this, be sure to configure a correct and valid IP address. If this attribute is not manually configured, the switch will automatically select the IP address of the VLAN interface as the NAS-IP address.

1.2.1 Configuring User Re-authentication at Reboot

Table 1-2 Configure user re-authentication at reboot

Operation	Command	Description
Enter system view	**system-view**	—
Enter RADIUS scheme view	**radius scheme** *radius-scheme-name*	—
Enable user re-authentication at reboot	**accounting-on enable** [**send** *times* | **interval** *interval*]	Optional By default, this feature is disabled. When this feature is enabled, the system can send the Accounting-On packet at most 15 times at intervals of three seconds by default.

1.2.2 Configuration Example for User Re-authentication at Reboot

I. Network requirements

Enable user re-authentication at reboot.

II. Configuration procedure

Enter system view.

```
<Quidway> system-view
```

Enter the view of the RADIUS scheme named CAMS (supposing this scheme has already existed).

```
[Quidway] radius scheme CAMS
```

Enable user re-authentication at reboot.

```
[Quidway-radius-CAMS] accounting-on enable
```

1.3 Tag VLAN Assignment on Trunk/Hybrid Port Supported by 802.1x Authentication

Currently, the 802.1x authentication module supports Tag VLAN assignment only on Access port. But some applications (for example, this kind of connection: switch—IP phone—PC) needs 802.1x authentication on Trunk/Hybrid port. For this reason, a new feature, Tag VLAN assignment on Trunk/Hybrid port, is designed.

- After a MAC address authentication succeeds, the address information is synchronously assigned in the whole fabric.

- When a user logs off, the system restores the original VLAN information on the Trunk/Hybrid port and synchronously deletes the corresponding address information from the whole fabric.

1.4 Identifier Authentication Method Attribute in RADIUS

The purpose of adding identifier authentication method attribute into RADIUS authentication packets is to distinguish different access modes, such as Portal, 802.1x, and PPPoE. For the non-Huawei client block function, you can limit its operation range to only 802.1x authentication, that is, allow the function to take effect only when the identifier authentication method attribute is 802.1x.

The adding of identifier authentication method attribute into an RADIUS authentication packet is to fill the Framed Protocol attribute in the RADIUS authentication request packet based on the access mode of the user.

1.5 Dynamic VLAN Assignment

Through dynamic VLAN assignment, the Ethernet switch dynamically adds the ports of the successfully authenticated users to different VLANs depending on the attribute values assigned by RADIUS server, so as to control the network resources the users can access.

Currently, the switch supports the following two data types of VLAN IDs assigned by RADIUS authentication server:

- Integer: The switch adds the port to a VLAN depending on the integer type of VLAN ID assigned by the RADIUS authentication server. If the VLAN does not exist, the switch creates the VLAN, and then adds the port to the new VLAN.
- String: The switch compares the character string type of VLAN ID assigned by the RADIUS authentication server with the existing VLAN names on it. If the switch finds a match, it adds the port to the corresponding VLAN; otherwise the VLAN assignment fails and the user fails to pass the authentication.

In actual application, to cooperate with Guest VLAN, port control is usually set to the port-based mode. If it is set to the MAC address–based mode, each port can have only one user end connected.

1.5.1 Configuring Dynamic VLAN Assignment

Table 1-3 Configure dynamic VLAN assignment

Operation	Command	Description
Enter system view	**system-view**	—
Create an ISP domain and enter its view	**domain** *isp-name*	—

Operation	Command	Description
Set the VLAN assignment mode to integer	**vlan-assignment-mode integer**	By default, this mode is integer.
Set the VLAN assignment mode to string	**vlan-assignment-mode string**	You must perform one of the two operations (this one and the above one)
Create a VLAN and enter its view	**vlan** *vlan_id*	—
Set a name for the assigned VLAN	**name** *string*	This operation is required when the VLAN assignment mode is set to string.

Caution:

- In string mode, if the VLAN name assigned by the RADIUS server is a string that contains only digital characters (for example, 1024) and the string can be transformed to an integer number in the valid VLAN range, the switch transforms this string to an integer number and adds the authenticated port to the VLAN whose ID is this number (VLAN 1024, for example).
- If you want to implement the dynamic VLAN assignment function on a port where both MSTP multi-instance and 802.1x is enabled, you must set the MSTP port to an edge port.

1.5.2 Configuration Example for Dynamic VLAN Assignment

I. Network requirements

- The RADIUS authentication server (in this example, a Windows IAS server) assigns a string type of VLAN ID (test).
- The VLAN name corresponding to this assigned VLAN ID is vlan 100.
- It is required that the switch adds the port to vlan 100 when test is assigned by the RADIUS server.

II. Network diagram

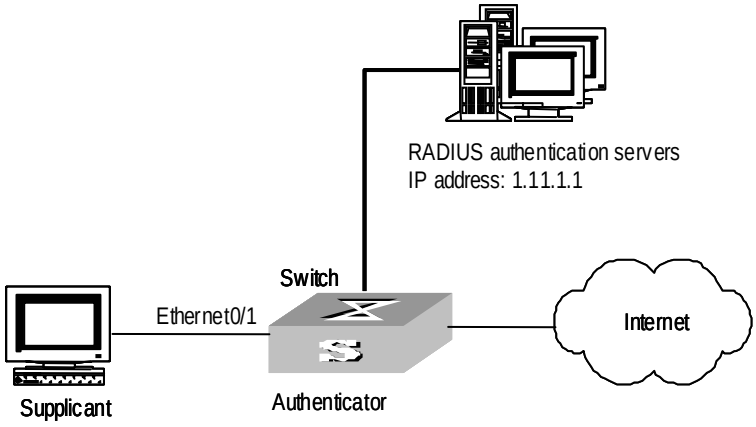

Figure 1-2 Network diagram for dynamic VLAN assignment

III. Configuration procedure

1) Create a RADIUS scheme.

```
[Quidway] radius scheme ias
[Quidway-radius-ias] primary authentication 1.11.1.1
[Quidway-radius-ias] primary accounting 1.11.1.1
[Quidway-radius-ias] key authentication hello
[Quidway-radius-ias] key accounting hello
[Quidway-radius-ias] quit
```

2) Create an ISP domain and reference the created RADIUS scheme in the domain.

```
[Quidway] domain ias
[Quidway-isp-ias] radius-scheme ias
```

Configure the VLAN assignment mode to string and return to the system view.

```
[Quidway-isp-ias] vlan-assignment-mode string
[Quidway-isp-ias] quit
```

3) Create a VLAN and specify a name for the VLAN.

```
[Quidway] vlan 100
```

Set the name of the assigned VLAN to test.

```
[Quidway-vlan100] name test
```

Chapter 2 New AAA&Radius Features Commands

2.1 New AAA&Radius Features Commands

2.1.1 accounting

Syntax

accounting { **none** | **radius-scheme** *radius-scheme-name* }

undo accounting

View

ISP domain view

Parameter

none: Specifies not to perform accounting.

radius-scheme-name: Name of a RADIUS scheme, a character string with no more than 32 characters.

Description

Use the **accounting** command to configure an accounting scheme for the current ISP domain.

Use the **undo accounting** command to cancel the accounting scheme configuration of the current ISP domain.

By default, no accounting scheme is configured for the ISP domain.

When you use the **accounting** command to specify a RADIUS scheme to be referenced by the current ISP domain, the RADIUS scheme must has already been defined.

If the **accounting** command is executed in an ISP domain view, the system uses the accounting scheme specified in this command to charge the users in the domain. Otherwise, the system uses the scheme specified in the **scheme** command to charge the users.

For related configuration, refer to the **scheme** and **radius scheme** commands in the security module of the *Quidway S5600 Series Ethernet Switches Command manual*.

Example

Enter system view.

```
<Quidway> system-view
```

Create an ISP domain named aabbcc.net.

```
[Quidway] domain aabbcc.net
New Domain added.
```

Specify the scheme radius as the RADIUS accounting scheme that will be referenced by the current ISP domain aabbcc.net.

```
[Quidway-isp-aabbcc.net] accounting radius-scheme radius
```

2.1.2 accounting-on enable

Syntax

accounting-on enable [**send** *times* | **interval** *interval*]

undo accounting-on { **enable** | **send** | **interval** }

View

RADIUS scheme view

Parameter

times: Maximum times to send Accounting-On packet, ranging from 1 to 256 and defaulting to 15.

interval: Interval to send Accounting-On packet, ranging from 1 to 30 and defaulting to 3 (in seconds).

Description

Use the **accounting-on enable** command to enable user re-authentication at reboot.

Use the **undo accounting-on enable** command to disable user re-authentication at reboot and restore the default interval and maximum times to transmit Accounting-On packet.

Use the **undo accounting-on send** command to restore the default maximum times to transmit Accounting-On packet.

Use the **undo accounting-on interval** command to restore the default interval to transmit Accounting-On packet.

By default, this feature is disabled.

The purpose of this feature is to resolve the following problem: users cannot re-log onto the network after the switch reboots because they are already online. After this feature is enabled, every time the switch reboots:

- The switch generates an Accounting-On packet, which mainly contains the following information: NAS-ID, NAS-IP (source IP address), and session ID.
- The switch sends the Accounting-On packet to the CAMS at regular intervals.
- Once the CAMS receives the Accounting-On packet, it sends a response to the switch. At the same time it finds and deletes the existing online information of the

user who was accessing the network through the switch before the reboot based on the NAS-ID, NAS-IP and session ID contained in the Accounting-On packet, and ends the charging of the user according to the last accounting update packet.

- Once the switch receives the response from the CAMS, it stops sending other Accounting-On packets.
- If the switch has tried the set maximum times to transmit the Accounting-On packet but still does not receive any response from the CAMS, it stops the sending of the Accounting-On packet.

Note:

The switch can automatically generate the main attributes (NAS-ID, NAS-IP and session ID) of the Accounting-On packets. However, you can also manually configure the NAS-IP attribute with the **nas-ip** command. When doing this, be sure to configure a correct and valid IP address. If this attribute is not configured manually, the switch will automatically select the IP address of the VLAN interface as the NAS-IP address.

For related configuration, refer to the **nas-ip** command in the security module of the *Quidway S5600 Series Ethernet Switches Command manual*.

Example

Enter system view.

```
<Quidway> system-view
```

Enter the view of the RADIUS scheme named CAMS (supposing this scheme has already existed).

```
[Quidway] radius scheme CAMS
```

Enable user re-authentication at reboot.

```
[Quidway-radius-CAMS] accounting-on enable
```

2.1.3 authentication

Syntax

authentication { **radius-scheme** *radius-scheme-name* [**local**] | **local** | **none** }

undo authentication

View

ISP domain view

Parameter

radius-scheme *radius-scheme-name*: Specifies a RADIUS authentication scheme.

local: Specifies to use local authentication scheme.

none: Specifies not to perform authentication.

Description

Use the **authentication** command to configure an authentication scheme for the current ISP domain.

Use the **undo authentication** command to restore the default authentication scheme of the current ISP domain.

By default, no separate authentication scheme is configured.

Before you use the **authentication** command to specify a RADIUS scheme to be referenced by the current ISP domain, the specified RADIUS scheme must has already been defined.

- After the **authentication radius-scheme** *radius-scheme-name* **local** command is executed, the **local** scheme is used as the secondary authentication scheme in case the RADIUS server does not respond normally. That is, if the communication between the switch and the RADIUS server is normal, no local authentication is performed; otherwise, local authentication is performed.
- After the **authentication local** command is executed, the **local** scheme is used as the primary scheme. In this case, only local authentication is performed. After the **authentication none** command is executed, no authentication is performed.
- After the **authentication** command is executed in an ISP domain view, the system uses the authentication scheme specified in the command to authenticate the users in the domain. Otherwise the system uses the scheme specified in the **scheme** command to authenticate the users.

For related configuration, refer to the **scheme** and **radius scheme** commands in the security module of the *Quidway S5600 Series Ethernet Switches Command manual*.

Example

Enter system view.

```
<Quidway> system-view
```

Create an ISP domain named aabbcc.net.

```
[Quidway] domain aabbcc.net
New Domain added.
```

Specify the scheme radius as the RADIUS authentication scheme to be referenced by the current ISP domain aabbcc.net.

```
[Quidway-isp-aabbcc.net] authentication radius-scheme radius
```

2.1.4 authorization

Syntax

authorization none

undo authorization

View

ISP domain view

Parameter

None

Description

Use the **authorization none** command to allow users in the current ISP domain to use network services without being authorized.

Use the **undo authorization** command to restore the default authorization scheme of the ISP domain.

By default, no separate authorization scheme is configured.

For related configuration, refer to the **scheme** and **radius scheme** commands in the security module of the *Quidway S5600 Series Ethernet Switches Command manual*.

Example

Enter system view.

```
<Quidway> system-view
```

Create an ISP domain named aabbcc.net.

```
[Quidway] domain aabbcc.net
New Domain added.
```

Allow users in the current ISP domain aabbcc.net to use network services without being authorized.

```
[Quidway-isp-aabbcc.net] authorization none
```

2.1.5 name

Syntax

name *string*

undo name

View

VLAN view

Parameter

string: Name of the assigned VLAN, a character string of no more than 32 characters.

Description

Use the **name** command to set a name for the assigned VLAN.

Use the **undo name** command to delete the name of the assigned VLAN.

By default, the VLAN ID (like VLAN 0001) is used as the name of the assigned VLAN.

This command is used for the dynamic VLAN assignment function. For the description of this function, refer to the **vlan-assignment-mode** command.

Related command: **dot1x guest-vlan** and **vlan-assignment-mode**.

Example

Set the name of VLAN 100 to test.

```
[Quidway] vlan 100
[Quidway-vlan100] name test
```

2.1.6 vlan-assignment-mode

Syntax

vlan-assignment-mode { **integer** | **string** }

View

ISP domain view

Parameter

integer: Set the VLAN assignment mode to integer.

string: Set the VLAN assignment mode to string.

Description

Use the **vlan-assignment-mode** command to configure the VLAN assignment mode.

By default, the VLAN assignment mode is integer. That is, the switch supports the integer type of VLAN IDs assigned by RADIUS authentication server.

Through dynamic VLAN assignment, the Ethernet switch dynamically adds the ports of the successfully authenticated users to different VLANs depending on the attribute values assigned by RADIUS server, so as to control the network resources the users can access.

In actual application, to cooperate with Guest VLAN, port control is usually set to the port-based mode. If it is set to the MAC address–based mode, each port can have only one user end connected.

Currently, the switch supports the following two data types of VLAN ID assigned by RADIUS authentication server:

- Integer: The switch adds the port to a VLAN depending on the integer type of VLAN ID assigned by the RADIUS authentication server. If the VLAN does not exist, the switch creates the VLAN, and then adds the port to the new VLAN.
- String: The switch compares the character string type of VLAN ID assigned by the RADIUS authentication server with the existing VLAN names on it. If the switch finds a match, it adds the port to the corresponding VLAN; otherwise the VLAN assignment fails and the user fails to pass the authentication.

Note:

In string mode, the switch processes an assigned VLAN ID in this way: If the VLAN name assigned by the RADIUS server is a string that contains only digital characters (for example, 1024) and the string can be transformed to an integer number in the valid VLAN range, the switch transforms this string to an integer number and adds the authenticated port to the VLAN whose ID is this number (VLAN 1024, for example).

Related command: **name** and **dot1x guest-vlan**.

Example

Set the VLAN assignment mode to string.

```
[Quidway-isp-huawei163.net] vlan-assignment-mode string
```