

Chapter 1 Centralized MAC Address Authentication Configuration.....	1-1
1.1 Introduction to Centralized MAC Address Authentication	1-1
1.2 Centralized MAC Address Authentication Configuration.....	1-2
1.2.1 Enabling Global/Port-based Centralized MAC Address Authentication.....	1-2
1.2.2 Configuring Centralized MAC Address Authentication Mode	1-2
1.2.3 Configuring the User Name and Password for Fixed Mode	1-3
1.2.4 Configuring an ISP Domain for MAC Address Authentication Users.....	1-3
1.2.5 Setting Centralized MAC Address Authentication Timers	1-3
1.3 Displaying and Debugging Centralized MAC Address Authentication	1-4
1.4 Centralized MAC Address Authentication Configuration Example.....	1-5
Chapter 2 Centralized MAC Address Authentication Configuration Commands.....	2-1
2.1 Centralized MAC Address Authentication Configuration Commands	2-1
2.1.1 debugging mac-authentication event	2-1
2.1.2 display mac-authentication.....	2-1
2.1.3 mac-authentication	2-3
2.1.4 mac-authentication authmode.....	2-5
2.1.5 mac-authentication authpassword	2-6
2.1.6 mac-authentication authusername.....	2-7
2.1.7 mac-authentication domain	2-7
2.1.8 mac-authentication timer	2-8

Table of Contents

Chapter 1 Centralized MAC Address Authentication Configuration.....	1-1
1.1 Introduction to Centralized MAC Address Authentication	1-1
1.2 Centralized MAC Address Authentication Configuration.....	1-2
1.2.1 Enabling Global/Port-based Centralized MAC Address Authentication.....	1-2
1.2.2 Configuring Centralized MAC Address Authentication Mode	1-2
1.2.3 Configuring the User Name and Password for Fixed Mode	1-3
1.2.4 Configuring an ISP Domain for MAC Address Authentication Users.....	1-3
1.2.5 Setting Centralized MAC Address Authentication Timers	1-3
1.3 Displaying and Debugging Centralized MAC Address Authentication	1-4
1.4 Centralized MAC Address Authentication Configuration Example.....	1-5
Chapter 2 Centralized MAC Address Authentication Configuration Commands.....	2-1
2.1 Centralized MAC Address Authentication Configuration Commands	2-1
2.1.1 debugging mac-authentication event	2-1
2.1.2 display mac-authentication.....	2-1
2.1.3 mac-authentication	2-3
2.1.4 mac-authentication authmode.....	2-5
2.1.5 mac-authentication authpassword	2-6

2.1.6 mac-authentication authusername.....	2-7
2.1.7 mac-authentication domain	2-7
2.1.8 mac-authentication timer.....	2-8

Chapter 1 Centralized MAC Address Authentication Configuration

1.1 Introduction to Centralized MAC Address Authentication

Centralized MAC address authentication controls accesses to a network through ports and MAC addresses. This kind of authentication requires no client software. When operating in centralized MAC address authentication mode, a switch begins to authenticate the user if it detects a new user MAC address.

Centralized MAC address authentication is implemented in the following two modes:

- MAC address mode. In this mode, user MAC address is used as both the user name and the password.
- Fixed mode. In this mode, user names and passwords are configured on the switch in advance. And users log on using the user names and passwords configured on the switch.

S5600 series Ethernet switches support local authentication and RADIUS server authentication.

- 1) When a RADIUS server is used for authentication, the switch serves as a RADIUS client. In this case, centralized MAC address authentications are carried out as follows.
 - In MAC address mode, a switch sends newly detected MAC addresses to the RADIUS server as both the user names and passwords. The rest handling procedures are the same as that of 802.1x.
 - In fixed mode, a switch sends the user names and passwords configured for fixed mode on it to the RADIUS server. It also inserts user MAC addresses into the calling-station-id fields of the RADIUS packets sent to the RADIUS server. The rest handling procedures are the same as that of 802.1x.
 - The RADIUS server authenticates the user and grants the user the permission to access the network if the user passes the authentication.
- 2) When local authentication is used, users are authenticated by the switch. When configuring local authentication, note that:
 - For MAC address authentication mode, you need to provide MAC addresses as the user names and passwords. (The MAC addresses provided here need to be in the format of xx-xx-xx-xx-xx-xx, where the character x stands for a hexadecimal number ranging from 0 to f.)
 - For fixed mode, configure the user name and password as those for fixed mode.
 - Set local service type as LAN-access.

1.2 Centralized MAC Address Authentication Configuration

The following sections describe centralized MAC address authentication configuration tasks:

- [Enabling Global/Port-based Centralized MAC Address Authentication](#)
- [Configuring Centralized MAC Address Authentication Mode](#)
- [Configuring the User Name and Password for Fixed Mode](#)
- [Configuring an ISP Domain for MAC Address Authentication](#)
- [Setting Centralized MAC Address Authentication Timers](#)

Note:

For a port, the centralized MAC address authentication configuration and the maximum number of learned MAC addresses configuration are mutually exclusive. That is, if you enable the centralized MAC address authentication function for a port, the maximum number of learned MAC addresses configuration (see the **mac-address max-mac-count** command) is unavailable. And if you set the maximum number of learned MAC addresses, the centralized MAC address authentication configuration is unavailable.

1.2.1 Enabling Global/Port-based Centralized MAC Address Authentication

[Table 1-1](#) lists the operations to enable centralized MAC address authentication on specified ports.

Table 1-1 Enable/disable centralized MAC address authentication

Operation	Command	Description
Enter system view	system-view	—
Enable centralized MAC address authentication	mac-authentication interface interface-list	Required By default, global and port-based centralized MAC address authentications are disabled.

Port-based centralized MAC address authentication configurations take effect only when global centralized MAC address authentication is also enabled.

1.2.2 Configuring Centralized MAC Address Authentication Mode

[Table 1-2](#) lists the operations to configure centralized MAC address authentication mode.

Table 1-2 Configure centralized MAC address authentication mode

Operation	Command	Description
Enter system view	system-view	—
Configure centralized MAC address authentication mode	mac-authentication authmode { usernameasmacaddress usernamefixed }	Optional By default, the authentication mode is MAC address mode.

1.2.3 Configuring the User Name and Password for Fixed Mode

If you configure the centralized MAC address authentication mode to be fixed mode, you need to configure the user name and password for fixed mode.

Table 1-3 Configure the user name and password for fixed mode

Operation	Command	Description
Enter system view	system-view	—
Configure a user name for fixed mode	mac-authentication authusername <i>username</i>	Optional By default, the user name is mac and the password is not required.
Configure the password for fixed mode	mac-authentication authpassword <i>password</i>	Required

1.2.4 Configuring an ISP Domain for MAC Address Authentication Users

Table 1-4 lists the operations to configure an ISP domain for centralized MAC address authentication users.

Table 1-4 Configure an ISP domain for MAC address authentication users

Operation	Command	Description
Enter system view	system-view	—
Configure an ISP domain for MAC address authentication users	mac-authentication domain <i>isp-name</i>	Required By default, the ISP domain is not configured for MAC address authentication users.

1.2.5 Setting Centralized MAC Address Authentication Timers

Following timers are used in centralized MAC address authentication.

- Offline-detect timer. This timer sets the interval for a switch to test whether or not a user goes offline. Upon determining a user is offline, a switch notifies the RADIUS server of the state of the user, and the RADIUS server in turn stops perform accounting operation on the user.
- Quiet timer. If a user fails to pass the authentication performed by a switch, the switch stops authenticating users for a specified period before it authenticates users again. You can use the quiet timer to set the period.
- Server-timeout timer. If the connection between a switch and a RADIUS server times out when the switch authenticates a user on one of its ports, the switch turns down the user. You can use the server-timeout timer to set the time out time.

Table 1-5 lists the operations to set centralized MAC address authentication timers.

Table 1-5 Set a centralized MAC address authentication timer

Operation	Command	Description
Enter system view	system-view	—
Set a centralized MAC address authentication timer	mac-authentication timer { offline-detect <i>offline-detect-value</i> quiet <i>quiet-value</i> server-timeout <i>server-timeout-value</i> }	Optional By default, the three MAC address authentication timers are set as follows: <ul style="list-style-type: none">• Offline-detect timer: 300 seconds• Quiet timer: 1 minute• Server-timeout timer: 100 seconds

1.3 Displaying and Debugging Centralized MAC Address Authentication

You can display and verify centralized MAC address authentication-related configuration by executing the **display** command in any view.

Table 1-6 Display and debug centralized MAC address authentication

Operation	Command	Description
Display global information about centralized MAC address authentication	display mac-authentication [interface <i>interface-list</i>]	Optional You can execute the display command in any view.

1.4 Centralized MAC Address Authentication Configuration Example

Note:

The configuration of centralized MAC address authentication is the same as that of 802.1x in this example except that:

- Centralized MAC address authentication is enabled both globally and for the ports.
 - For MAC address mode, the user name and password of a user to be authenticated locally need to be configured as the MAC address of the user.
 - For MAC address mode, the user name and password of a user to be authenticated by a RADIUS server need to be configured as the MAC address of the user on the RADIUS server.
-

The following section describes how to enable port-based and global centralized MAC address authentication, and local user configuration.

Enable centralized MAC address authentication on GigabitEthernet1/0/2 port.

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

```
[Quidway] mac-authentication interface GigabitEthernet 1/0/2
```

Configure centralized MAC address authentication mode to be MAC address mode.

```
[Quidway] mac-authentication authmode usernameasmacaddress
```

Add a local access user.

- Configure the user name and password for the local user.

```
[Quidway] local-user 00-e0-fc-01-01-01
```

```
[Quidway-luser-00-e0-fc-01-01-01] password simple 00-e0-fc-01-01-01
```

- Set service type to LAN-access for the local user.

```
[Quidway-luser-00-e0-fc-01-01-01] service-type lan-access
```

Enable global centralized MAC address authentication.

```
[Quidway] mac-authentication
```

Configure the domain name for centralized MAC address authentication user to be aabbcc163.net.

```
[Quidway] mac-authentication domain aabbcc163.net
```

For domain-related configuration, refer to the configuration example in the chapter concerning 802.1x of this manual.

Chapter 2 Centralized MAC Address Authentication Configuration Commands

2.1 Centralized MAC Address Authentication Configuration Commands

2.1.1 debugging mac-authentication event

Syntax

debugging mac-authentication event
undo debugging mac-authentication event

View

User view

Parameter

None

Description

Use the **debugging mac-authentication event** command to enable debugging for centralized MAC address authentication events.

Use the **undo debugging mac-authentication event** command to disable debugging for centralized MAC address authentication events.

Example

Enable debugging for centralized MAC address authentication events.

```
<Quidway> debugging mac-authentication event
```

2.1.2 display mac-authentication

Syntax

display mac-authentication [interface *interface-list*]

View

Any view

Parameter

interface-list: Lists of Ethernet ports. You can specify multiple Ethernet ports by providing this argument in the form of *interface-list* = { *interface-type interface-number* [*to interface-type interface-number*] } &<1-10>, where &<1-10> means that you can provide up to 10 port indexes/port index lists for this argument.

Description

Use the **display mac-authentication** command to display the global information about centralized MAC address authentication, including the state of centralized MAC address authentication (enabled or disabled), values of centralized MAC address authentication timers, the number of online users, MAC addresses during quiet period, and MAC authentication information about each port.

Example

Display the global information about centralized MAC address authentication.

```
<Quidway> display mac-authentication
mac address authentication is Enabled.
authentication mode is UsernameAsMacAddress
Fixed username:mac
Fixed password:not configured
    offline detect period is 300s
    quiet period is 1 minute(s).
    server response timeout value is 100s
    max allowed user number is 1024
    current user number amounts to 0
    current domain: not configured, use default domain
Silent Mac User info:
    MAC ADDR          From Port          Port Index
GigabitEthernet1/0/1 is link-up
    MAC address authentication is Enabled
    Authenticate success: 0, failed: 0
    Current online user number is 0
    MAC ADDR          Authenticate state    AuthIndex
... (omitted)
```

Table 2-1 Description on the fields of the **display mac-authentication** command

Field	Description
mac address authentication is Enabled	Centralized MAC address authentication is enabled.
authentication mode	Centralized MAC address authentication mode. The default is MAC address mode.

Field	Description
the Fixed username	User name of fixed mode. The default is mac.
the Fixed password	Password of fixed mode. It is not configured by default.
offline detect period	The offline-detect timer value. The timer sets the interval for a switch to check whether a user goes offline and is set to 300 seconds by default.
quiet period	Quiet timer value. The timer sets the quiet period and is set to 1 minute by default.
server response timeout value	Server-timeout timer value. The timer sets the timeout time for the connection between the switch and the RADIUS server and is set to 100 seconds by default.
max allowed user number	The maximum number of users supported by the switch, which defaults to 1,024.
current user number amounts to	The number of current users
current domain	The current domain, which is not configured by default.
Silent Mac User info	The information about the quiet user information. When a user fails to pass MAC address authentication because of incorrect user name or password input, the switch sets the user to be in quiet state. During quiet period, the switch does not authenticate this user.
GigabitEthernet1/0/1 is link-up	The link GigabitEthernet1/0/1 port connected to is up.
MAC address authentication is Enabled	MAC address authentication is enabled on GigabitEthernet1/0/1 port.
Authenticate success: 0, failed: 0	MAC address authentication statistics of the ports, including the times of successful and failed authentication.
Current online user number	The number of current online users
Authenticate state	User state, which can be: CONNECTING: Connecting SUCCESS: Authenticated FAILURE: Fail to pass authentication LOGOFF: Offline.

2.1.3 mac-authentication

Syntax

mac-authentication [**interface** *interface-list*]

undo mac-authentication [interface *interface-list*]

View

System view, Ethernet port view

Parameter

interface-list: Lists of Ethernet ports. You can specify multiple Ethernet ports by providing this argument in the form of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, where &<1-10> means that you can provide up to 10 port indexes/port index lists for this argument.

Description

Use the **mac-authentication** command to enable centralized MAC address authentication globally (current device) or on specified ports.

Use the **undo mac-authentication** command to disable centralized MAC address authentication globally or on specified ports.

By default, centralized MAC address authentication is disabled both globally and on any port.

When being executed in system view, the **mac-authentication** command enables centralized MAC address authentication globally if you do not provide the *interface-list* argument, otherwise, the command enables centralized MAC address authentication on the specified ports. When being executed in Ethernet port view, the command enables centralized MAC address authentication on the current port only. In this case, the *interface-list* is unnecessary.

You can configure centralized MAC address authentication-related parameters no matter whether or not centralized MAC authentication is enabled. If you do not configure the parameters before enabling centralized MAC address authentication globally, the default parameters are adopted.

Note:

- To make the configuration of port-based centralized MAC address authentication take effect, you must enable global centralized MAC address authentication globally besides enabling port-based centralized MAC address authentication.
 - For a port, the centralized MAC address authentication configuration and the maximum number of learned MAC addresses configuration are mutually exclusive. That is, if you enable the centralized MAC address authentication function for a port, the maximum number of learned MAC addresses configuration (see the **mac-address max-mac-count** command) is unavailable. And if you set the maximum number of learned MAC addresses, the centralized MAC address authentication configuration is unavailable.
-

Example

Enable centralized MAC address authentication on GigabitEthernet 1/0/1 port.

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

System View: return to User View with Ctrl+Z.

```
[Quidway] mac-authentication interface GigabitEthernet 1/0/1
```

Enable centralized MAC address authentication feature globally.

```
[Quidway] mac-authentication
```

2.1.4 mac-authentication authmode**Syntax**

mac-authentication authmode { usernameasmacaddress | usernamefixed }

undo mac-authentication authmode

View

System view

Parameter

usernameasmacaddress: Authenticates users in MAC address mode.

usernamefixed: Authenticates users in fixed mode.

Description

Use the **mac-authentication authmode** command to set MAC address authentication mode.

Use the **undo mac-authentication authmode** command to cancel the configured MAC address authentication mode.

- The **usernameasmacaddress** keyword specifies to authenticate users in MAC address mode. That is, the MAC address of a user is used as both the user name and password.
- The **usernamefixed** keyword specifies to authenticate users in fixed mode, where you need to configure both user name and password separately.

By default, a switch authenticates users in MAC address mode.

Example

Configure to authenticate users in fixed mode.

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

System View: return to User View with Ctrl+Z.

```
[Quidway] mac-authentication authmode usernamefixed
```

2.1.5 mac-authentication authpassword

Syntax

mac-authentication authpassword *password*

undo mac-authentication authpassword

View

System view

Parameter

password: Password for authentication, a string comprising of 1 to 63 characters.

Description

Use the **mac-authentication authpassword** command to set a password when a switch authenticates users in fixed mode.

Use the **undo mac-authentication authpassword** command to remove the configured password.

By default, no password is configured for the fixed mode of MAC address authentication.

Example

Set the password to mac for fixed mode.

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

System View: return to User View with Ctrl+Z.

```
[Quidway] mac-authentication authpassword mac
```


2.1.6 mac-authentication authusername

Syntax

mac-authentication authusername *username*

undo mac-authentication authusername

View

System view

Parameter

username: User name for authentication, a string comprising of 1 to 55 characters.

Description

Use the **mac-authentication authusername** command to set a user name when a switch authenticates users in fixed mode.

Use the **undo mac-authentication authusername** command to restore the default user name.

By default, the user name is mac.

Example

Set the user name to vipuser for fixed mode.

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

System View: return to User View with Ctrl+Z.

```
[Quidway] mac-authentication authusername vipuser
```

Restore the default user name.

```
[Quidway] undo mac-authentication authusername
```

2.1.7 mac-authentication domain

Syntax

mac-authentication domain *isp-name*

undo mac-authentication domain

View

System view

Parameter

isp-name: ISP domain name, a string comprising up to 24 characters. Note that this argument cannot contain "/", ".", "*", "?", "<", and ">".

Description

Use the **mac-authentication domain** command to configure an ISP domain for centralized MAC address authentication users.

Use the **undo mac-authentication domain** command to restore the default ISP domain.

By default, the domain for centralized MAC address authentication users is not configured.

Example

Configure the domain for centralized MAC address authentication users to be Cams.

```
<Quidway> system-view
System View: return to User View with Ctrl+Z.
[Quidway] mac-authentication domain Cams
```

2.1.8 mac-authentication timer

Syntax

mac-authentication timer { **offline-detect** *offline-detect-value* | **quiet** *quiet-value* | **server-timeout** *server-timeout-value* }

undo mac-authentication timer { **offline-detect** | **quiet** | **server-timeout** }

View

System view

Parameter

offline-detect *offline-detect-value*: Sets the offline-detect timer (in seconds). This timer sets the interval for a switch to test whether or not a user goes offline. The *offline-detect-value* argument ranges from 1 to 65,535 and defaults to 300.

quiet *quiet-value*: Specifies the quiet timer. If a user fails to pass the authentication performed by a switch, the switch stops authenticating users for a period specified by the *quiet-value* before it authenticates users again. The *quiet-value* argument ranges from 1 to 65,535 (in minutes) and defaults to 1.

server-timeout *server-timeout-value*: Specifies the server-timeout timer. If the connection between a switch and a RADIUS server times out when the switch authenticates a user on one of its ports, the switch turns down the user. The *server-timeout-value* argument ranges from 1 to 65,535 (in seconds) and defaults to 100.

Description

Use the **mac-authentication timer** command to set centralized MAC address authentication timers.

Use the **undo mac-authentication timer** command to restore the default centralized MAC address authentication timers.

Related command: **display mac-authentication**.

Example

Set the server-timeout timer to 150 seconds.

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

System View: return to User View with Ctrl+Z.

```
[Quidway] mac-authentication timer server-timeout 150
```