

# 目 录

1 MAC地址认证配置命令 .....	1-1
1.1 MAC地址认证配置命令 .....	1-1
1.1.1 display mac-authentication .....	1-1
1.1.2 mac-authentication .....	1-3
1.1.3 mac-authentication domain .....	1-4
1.1.4 mac-authentication guest-vlan .....	1-5
1.1.5 mac-authentication max-user .....	1-6
1.1.6 mac-authentication timer .....	1-6
1.1.7 mac-authentication user-name-format .....	1-7
1.1.8 reset mac-authentication statistics .....	1-9

# 1 MAC地址认证配置命令

## 1.1 MAC地址认证配置命令

### 1.1.1 display mac-authentication

#### 【命令】

```
display mac-authentication [ interface interface-list ] [ | { begin | exclude | include } regular-expression ]
```

#### 【视图】

任意视图

#### 【缺省级别】

2: 系统级

#### 【参数】

**interface** *interface-list*: 端口列表，表示多个端口，表示方式为 *interface-list* = { *interface-type* *interface-number* [ **to** *interface-type* *interface-number* ] }&<1-10>。其中，*interface-type* 为端口类型，*interface-number* 为端口号。&<1-10>表示前面的参数最多可以输入 10 次。起始端口类型必须和终止端口类型一致，并且终止端口号必须大于起始端口号。

|: 使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

**begin**: 从包含指定正则表达式的行开始显示。

**exclude**: 只显示不包含指定正则表达式的行。

**include**: 只显示包含指定正则表达式的行。

*regular-expression*: 表示正则表达式，为 1~256 个字符的字符串，区分大小写。

#### 【描述】

**display mac-authentication** 命令用来显示 MAC 地址认证的相关信息，主要包括全局及端口的配置信息、认证报文统计信息以及认证用户信息。

需要注意的是：

- 如果指定参数 **interface** *interface-list*，则显示全局及指定端口上的 MAC 地址认证信息。
- 如果不指定任何参数，则显示全局及所有端口上的 MAC 地址认证信息。

#### 【举例】

# 显示 MAC 地址认证信息。

```
<Sysname> display mac-authentication
MAC address authentication is enabled.
User name format is MAC address in lowercase, like xxxxxxxxxxxxxx
Fixed username:mac
Fixed password:not configured
Offline detect period is 300s
```

```

Quiet period is 60s.
Server response timeout value is 100s
the max allowed user number is 2048 per slot
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
Max number of on-line users is 2048
Current online user number is 0
                MAC Addr           Authenticate state   Auth Index

```

..... (略)

表1-1 display mac-authentication 命令显示信息描述表

字段	描述
MAC address authentication is enabled	MAC 地址认证特性已经开启
User name format is MAC address in lowercase, like xxxxxxxxxxxx	<p>本字段用于显示 MAC 地址认证使用的用户名格式，有以下两种情况：</p> <ul style="list-style-type: none"> <li>若采用 MAC 地址形式，则显示具体的用户名格式以及是否带连字符、字母是否大小写，例如本例中“User name format is MAC address in lowercase, like xxxxxxxxxxxx”，它表示用户名格式为不带连字符的 MAC 地址，其中字母为小写。</li> <li>若采用固定用户名格式，则显示“User name format is fixed account”。</li> </ul>
Fixed username:	<p>固定用户名</p> <ul style="list-style-type: none"> <li>采用 MAC 地址格式时，该值显示为“mac”，无实际意义，仅表示采用 MAC 地址作为用户名和密码。</li> <li>采用固定用户名格式时，该值为配置的用户名（缺省为 mac）。</li> </ul>
Fixed password:	<p>固定用户名的密码</p> <ul style="list-style-type: none"> <li>采用 MAC 地址格式时，该值显示为“not configured”。</li> <li>采用固定用户名格式时，该值为配置的用户密码。</li> </ul>
Offline detect period	下线检测定时器的时间间隔
Quiet period	静默定时器的时间间隔
Server response timeout value	服务器连接超时定时器的值
The max allowed user number	设备每板最大支持的 MAC 地址认证用户数
Current user number amounts	当前用户数
Current domain: not configured, use default domain	当前认证域没有配置，使用缺省域
Silent Mac User info	静默用户信息
GigabitEthernet1/0/1 is link-up	端口 GigabitEthernet1/0/1 链路处于 UP 状态

字段	描述
MAC address authentication is enabled	端口 GigabitEthernet1/0/1MAC 地址认证特性已开启
Authenticate success: 0, failed: 0	端口上 MAC 地址认证的统计信息，包括认证通过和认证失败的数目
Max number of on-line users	端口最多可容纳的接入用户数 如果端口没有开启 MAC 地址认证，则显示 0
Current online user number	端口当前的接入用户数
MAC Addr	MAC 地址
Authenticate state	端口接入用户的状态，共有四种： <ul style="list-style-type: none"> <li>• MAC_AUTHENTICATOR_CONNECT：正在连接</li> <li>• MAC_AUTHENTICATOR_SUCCESS：认证通过</li> <li>• MAC_AUTHENTICATOR_FAIL：认证失败</li> <li>• MAC_AUTHENTICATOR_LOGOFF：已下线</li> </ul>
AuthIndex	认证体索引号

## 1.1.2 mac-authentication

### 【命令】

在系统视图下：

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

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

在以太网端口视图下：

**mac-authentication**

**undo mac-authentication**

### 【视图】

系统视图/以太网端口视图

### 【缺省级别】

2：系统级

### 【参数】

**interface** *interface-list*：以太网端口列表，表示多个以太网端口，表示方式为 *interface-list* = { *interface-type interface-number* [ **to** *interface-type interface-number* ] }&<1-10>。其中，*interface-type* 为端口类型，*interface-number* 为端口号。&<1-10>表示前面的参数最多可以输入 10 次。起始端口类型必须和终止端口类型一致，并且终止端口号必须大于起始端口号。

### 【描述】

**mac-authentication** 命令用来开启指定端口上或全局的 MAC 地址认证特性。**undo mac-authentication** 命令用来关闭指定端口上或全局的 MAC 地址认证特性。

缺省情况下，所有端口及全局的 MAC 地址认证特性都处于关闭状态。

需要注意的是：

- 在系统视图下使用该命令时，如果不输入可选项 **interface interface-list**，则表示开启全局的 MAC 地址认证特性；如果指定了 **interface interface-list**，则表示开启指定端口的 MAC 地址认证特性。
- 只有全局和端口的 MAC 地址认证特性均开启后，MAC 地址认证配置才能在端口上生效。

### 【举例】

# 开启全局的 MAC 地址认证特性。

```
<Sysname> system-view
[Sysname] mac-authentication
Mac-auth is enabled globally.
```

# 开启以太网端口 GigabitEthernet1/0/1 上的 MAC 地址认证特性。

```
<Sysname> system-view
[Sysname] mac-authentication interface gigabitethernet 1/0/1
Mac-auth is enabled on port GigabitEthernet1/0/1.
```

或者

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication
Mac-auth is enabled on port GigabitEthernet1/0/1.
```

## 1.1.3 mac-authentication domain

### 【命令】

**mac-authentication domain** *domain-name*

**undo mac-authentication domain**

### 【视图】

系统视图/以太网端口视图

### 【缺省级别】

2: 系统级

### 【参数】

*domain-name*: ISP 域名，为 1~24 个字符的字符串，不区分大小写，且不能包括 “/”、“:”、“\*”、“?”、“<”、“>” 以及 “@” 等特殊字符。

### 【描述】

**mac-authentication domain** 命令用来指定 MAC 地址认证用户使用的认证域。**undo mac-authentication domain** 命令用来恢复缺省情况。

缺省情况下，未指定 MAC 地址认证用户使用的认证域，使用系统缺省的认证域。缺省认证域的介绍请参见“安全命令参考/AAA”中的命令 **domain default enable**。

需要注意的是：

- 系统视图下指定的认证域对所有使能了 MAC 地址认证的端口生效。
- 以太网端口视图下指定的认证域仅对本端口有效。不同的端口可以指定不同的认证域。
- 端口上接入的 MAC 地址认证用户将按照如下先后顺序选择认证域：端口上指定的认证域-->系统视图下指定的认证域-->系统缺省的认证域。

相关配置可参见命令 **display mac-authentication**。

#### 【举例】

```
# 在系统视图下指定 MAC 地址认证用户使用的认证域为 domain1。
<Sysname> system-view
[Sysname] mac-authentication domain domain1
# 指定端口 GigabitEthernet1/0/1 上接入的 MAC 地址认证用户使用的认证域为 aabbcc。
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication domain aabbcc
```

### 1.1.4 mac-authentication guest-vlan

#### 【命令】

```
mac-authentication guest-vlan guest-vlan-id
undo mac-authentication guest-vlan
```

#### 【视图】

以太网端口视图

#### 【缺省级别】

2: 系统级

#### 【参数】

*guest-vlan-id*: 端口上指定的 Guest VLAN ID，取值范围为 1~4094。该 VLAN 必须已经创建。

#### 【描述】

**mac-authentication guest-vlan** 命令用来配置 MAC 地址认证的 Guest VLAN。如果配置生效，则所有经由该端口认证失败的用户，将被加入到指定的 Guest VLAN。**undo mac-authentication guest-vlan** 命令用来取消 MAC 地址认证的 Guest VLAN 配置。

缺省情况下，没有配置 MAC 地址认证的 Guest VLAN。

需要注意的是：

- 只有开启 MAC 认证特性的情况下，Guest VLAN 才能生效。
- 只有使能端口的 MAC VLAN 功能的情况下，Guest VLAN 才生效。
- 禁止删除已被配置为 Guest VLAN 的 VLAN，若要删除该 VLAN，请先使用命令 **undo mac-authentication guest-vlan** 取消 MAC 地址认证的 Guest VLAN 配置。
- 如果某个 VLAN 被指定为 Super VLAN，则该 VLAN 不能被指定为某个端口的 Guest VLAN；同样，如果某个 VLAN 被指定为某个端口的 Guest VLAN，则该 VLAN 不能被指定为 Super VLAN。关于 Super VLAN 的详细内容请参见“二层技术-以太网交换配置指导”中的“Super VLAN”。

相关配置可参考命令 **mac-authentication** 和“二层技术-以太网交换命令参考/VLAN”中的命令 **mac-vlan enable**。

#### 【举例】

```
# 配置以太网端口 GigabitEthernet1/0/1 的 MAC 地址认证的 Guest VLAN 为已经创建的 VLAN 5。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] mac-authentication guest-vlan 5
```

### 1.1.5 mac-authentication max-user

#### 【命令】

```
mac-authentication max-user user-number  
undo mac-authentication max-user
```

#### 【视图】

以太网端口视图

#### 【缺省级别】

2: 系统级

#### 【参数】

*user-number*: 端口同时可容纳接入用户数量的最大值，取值范围为 1~2048。

#### 【描述】

**mac-authentication max-user** 命令用来配置端口同时可容纳接入的 MAC 地址认证用户数量的最大值。**undo mac-authentication max-user** 命令用来恢复该值的缺省值。

缺省情况下，端口同时可容纳接入用户数量的最大值为 2048。

#### 【举例】

# 设置端口 GigabitEthernet1/0/1 最多同时可容纳 32 个 MAC 地址认证用户接入。

```
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] mac-authentication max-user 32
```

### 1.1.6 mac-authentication timer

#### 【命令】

```
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 }
```

#### 【视图】

系统视图

#### 【缺省级别】

2: 系统级

#### 【参数】

**offline-detect** *offline-detect-value*: 表示下线检测定时器。其中，*offline-detect-value* 表示下线检测定时器的值，取值范围 60~65535，单位为秒。

**quiet** *quiet-value*: 表示静默定时器。其中 *quiet-value* 表示静默定时器的值，取值范围 1~3600，单位为秒。

**server-timeout server-timeout-value:** 表示服务器超时定时器。其中，*server-timeout-value* 表示服务器超时定时器的值，取值范围为 100~300，单位为秒。

#### 【描述】

**mac-authentication timer** 命令用来配置 MAC 地址认证定时器。**undo mac-authentication timer** 命令用来将指定的定时器恢复为缺省情况。

缺省情况下，下线定时器的值为 300 秒，静默定时器的值为 60 秒，服务器的超时定时器的值为 100 秒。

MAC 地址认证过程受以下定时器的控制：

- 下线检测定时器（**offline-detect**）：用来设置用户空闲超时的时间间隔。如果在两个时间间隔之内，没有来自用户的流量通过，设备将切断用户的连接，同时通知 RADIUS 服务器，停止对该用户的计费。
- 静默定时器（**quiet**）：用来设置用户认证失败以后，设备需要等待的时间间隔。在静默期间，设备不对来自该用户的报文进行认证处理，直接丢弃。静默期后，如果设备再次收到该用户的报文，则依然可以对其进行认证处理。
- 服务器超时定时器（**server-timeout**）：用来设置设备同 RADIUS 服务器的连接超时时间。在用户的认证过程中，如果服务器超时定时器超时，设备将在相应的端口上禁止此用户访问网络。

相关配置可参考命令 **display mac-authentication**。

#### 【举例】

# 设置服务器超时定时器时长为 150 秒。

```
<Sysname> system-view
[Sysname] mac-authentication timer server-timeout 150
```

### 1.1.7 mac-authentication user-name-format

#### 【命令】

**mac-authentication user-name-format { fixed [ account name ] [ password { cipher | simple } password ] | mac-address [ { with-hyphen | without-hyphen } [ lowercase | uppercase ] ] }**

**undo mac-authentication user-name-format**

#### 【视图】

系统视图

#### 【缺省级别】

2: 系统级

#### 【参数】

**fixed:** 表示采用固定用户名格式。

**account name:** 指定发送给 RADIUS 服务器进行认证或者在本地进行认证的用户名。其中 *name* 为用户名，为 1~55 个字符的字符串，不区分大小写，缺省为 **mac**。

**password { cipher | simple } password:** 指定固定用户名的密码。其中，**cipher** 表示密文显示密码，**simple** 表示明文显示密码，*password* 表示用户密码。无缺省值。



- 密文显示的情况下，可输入 1~63 个字符的明文字符串密码，也可输入长度为 24 或 88 个字符的密文字符串密码；
- 明文显示的情况下，只能输入 1~63 个字符的明文字符串。

**mac-address:** 表示使用用户的 MAC 地址做为用户名和密码。

**with-hyphen:** 带连字符“-”的 MAC 地址格式，例如 xx-xx-xx-xx-xx-xx。

**without-hyphen:** 不带连字符“-”的 MAC 地址格式，例如 xxxxxxxxxxxx。

**lowercase:** MAC 地址中的字母为小写。

**uppercase:** MAC 地址中的字母为大写。

### 【描述】

**mac-authentication user-name-format** 命令用来配置 MAC 地址认证的用户名格式。**undo mac-authentication user-name-format** 命令用来恢复缺省情况。

缺省情况下，使用用户的 MAC 地址做用户名和密码，其中字母为小写，MAC 地址不带连字符“-”。需要注意的是：

- 若指定用户的 MAC 地址为用户名，则用户密码也为用户的源 MAC 地址。
- 在 **cipher** 方式下，长度小于等于 16 的明文密码会被加密为长度是 24 的密文，长度大于 16 且小于等于 63 的明文密码会被加密为长度是 88 的密文。当用户输入长度为 24 的密码时，如果密码能够被系统解密，则按密文密码处理；若不能被解密，则按明文密码处理。

相关配置可参考命令 **display mac-authentication**。

### 【举例】

# 配置 MAC 认证的用户名为 abc，密码是明文显示的 xyz。

```
<Sysname> system-view
[Sysname] mac-authentication user-name-format fixed account abc password simple xyz
[Sysname] display this
#
mac-authentication user-name-format fixed account abc password simple xyz
#
```

# 配置 MAC 认证的用户名为 abc，密码是密文显示的 xyz。

```
<Sysname> system-view
[Sysname] mac-authentication user-name-format fixed account abc password cipher xyz
[Sysname] display this
#
mac-authentication user-name-format fixed account abc password cipher 5Q4$,*^18
N'Q=^Q`MAF4<1!!
#
```

# 配置 MAC 认证的用户名为 abc，密码是密文显示的 5Q4\$,\*^18N'Q=^Q`MAF4<1!!。

```
<Sysname> system-view
[Sysname] mac-authentication user-name-format fixed account abc password cipher 5Q4$,*^18
N'Q=^Q`MAF4<1!!
```

# 配置用户的 MAC 地址为用户名和密码，使用带连字符“-”的 MAC 地址格式，其中字母大写。

```
<Sysname> system-view
[Sysname] mac-authentication user-name-format mac-address with-hyphen uppercase
```

## 1.1.8 reset mac-authentication statistics

### 【命令】

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

### 【视图】

用户视图

### 【缺省级别】

2: 系统级

### 【参数】

**interface** *interface-list*: 端口列表，表示多个端口，表示方式为 *interface-list* = { *interface-type interface-number* [ **to** *interface-type interface-number* ] }&<1-10>。其中，*interface-type* 为端口类型，*interface-number* 为端口号。&<1-10>表示前面的参数最多可以输入 10 次。起始端口类型必须和终止端口类型一致，并且终止端口号必须大于起始端口号。

### 【描述】

**reset mac-authentication statistics** 命令用来清除 MAC 认证的统计信息。

需要注意的是：

- 如果不指定端口类型和端口号，则清除设备上的全局及所有端口的 MAC 认证统计信息；
- 如果指定端口类型和端口号，则清除指定端口上的 MAC 认证统计信息。

相关配置可参考命令 **display mac-authentication**。

### 【举例】

# 清除以太网端口 GigabitEthernet1/0/1 上的 MAC 认证统计信息。

```
<Sysname> reset mac-authentication statistics interface gigabitethernet 1/0/1
```