目 录

1 MAC地址认证

1.1 MAC地址认证配置命令

1.1.1 display mac-authentication

display mac-authentication 命令用来显示 MAC 地址认证的相关信息。

【命令】

display mac-authentication [**interface** *interface-type interface-number*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

interface *interface-type interface-number*：显示全局及指定端口的 MAC 地址认证相关信息。*interface-type interface-number* 为端口类型和端口编号。若指定的端口上未使能 MAC 地址认证，则不显示该端口任何信息。

【使用指导】

如果不指定任何参数，则显示所有在线 MAC 地址认证的详细信息，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。

【举例】

显示 MAC 地址认证信息。

```
<Sysname> display mac-authentication
Global MAC authentication parameters:
   MAC authentication     : Enabled
   User name format       : MAC address in lowercase(xx-xx-xx-xx-xx-xx)
           Username       : mac
           Password       : Not configured
   Offline detect period  : 300 s
   Quiet period           : 60 s
   Server timeout         : 100 s
   Authentication domain  : Not configured, use default domain
 Online MAC-auth wired users    : 1
 Online MAC-auth wireless users : 2

 Silent MAC users:
         MAC address       VLAN ID  From port                  Port index

 AP name: fatap  Radio ID: 1  SSID: wlan_maca_ssid
```

```
  BSSID                     : 0023-ee00-1132
MAC authentication          : Enabled
  Authentication domain     : Not configured
  Max online users          : 256
  Authentication attempts   : successful 1, failed 0
```

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

字段	描述
Global MAC authentication parameters	全局MAC地址认证参数
MAC authentication	MAC地址认证的开启状态
User name format	MAC地址认证使用的账号格式 • 若采用 MAC 地址账号，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“MAC address in lowercase(xx-xx-xx-xx-xx-xx)”，它表示用户名格式为六段式的 MAC 地址，其中字母为小写 • 若采用固定用户名账号，则显示“Fixed account”
Username	用户名 • 采用 MAC 地址账号时，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 • 采用固定用户名账号时，该值为配置的用户名（缺省为 mac）
Password	用户名的密码 • 采用 MAC 地址账号时，该值显示为“Not configured” • 采用固定用户名账号时，配置的值将显示为******
Offline detect period	下线检测定时器的值
Quiet period	静默定时器的值
Server timeout	服务器连接超时定时器的值
Authentication domain	系统视图下指定的MAC地址认证用户使用的认证域，如果没有指定认证域，则显示Not configured, use default domain
Online MAC-auth wired users	在线有线用户和正在发起MAC地址认证的有线用户的总数
Online MAC-auth wireless users	在线无线用户和正在发起MAC地址认证的无线用户的总数
Silent MAC users	静默用户信息
MAC address	静默用户的MAC地址
VLAN ID	静默用户所在的VLAN
From port	静默用户接入的端口名称
Port index	静默用户接入的端口索引号
MAC authentication	当前端口的MAC地址认证开启状态
Authentication domain	端口上指定的MAC地址认证用户使用的认证域

字段	描述
Re-auth server-unreachable	重认证时服务器不可达对MAC地址认证的在线用户采取的动作 • Logoff：重认证服务器不可达，强制 MAC 地址认证在线用户下线 • Online：重认证服务器不可达，保持 MAC 地址认证在线用户在线
Max online users	本端口最多可容纳的接入用户数
Authentication attempts: successful 1, failed 0	端口上MAC地址认证的统计信息，包括认证通过的次数和认证失败的次数
MAC address	接入用户的MAC地址
Auth state	接入用户的状态 • Authenticated：认证成功 • Unauthenticated：认证失败
AP name	AP名称
Radio ID	Radio编号
SSID	服务集标识符
BSSID	基本服务集标识符

1.1.2 display mac-authentication connection

display mac-authentication connection 命令用来显示 MAC 地址认证在线用户的详细信息。

【命令】

display mac-authentication connection [**interface** *interface-type interface-number* | **user-mac** *mac-addr* | **user-name** *user-name*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

interface *interface-type interface-number*：显示指定端口的 MAC 地址认证用户信息。其中 *interface-type interface-number* 表示绑定的端口类型和端口编号。若不指定本参数，则显示设备上所有的 MAC 地址认证用户信息。

user-mac *mac-addr*：显示指定 MAC 地址的 MAC 地址认证用户信息。其中 *mac-addr* 表示用户的 MAC 地址，格式为 H-H-H。若不指定本参数，则显示设备上所有的 MAC 地址认证用户信息。

user-name *user-name*：显示指定用户名的 MAC 地址认证用户信息。其中 *user-name* 表示用户名（可包含域名），为 1～55 个字符的字符串，区分大小写。若不指定本参数，则显示设备上所有的 MAC 地址认证用户信息。

【使用指导】

如果不指定任何参数，则显示所有端口上的 MAC 地址认证在线用户信息。

【举例】

显示所有 MAC 地址认证在线用户信息。

```
<Sysname> display mac-authentication connection
Total connections: 1

User MAC address: 0015-e9a6-7cfe
Access interface: GigabitEthernet1/0/1
Username: ias
Authentication domain: h3c
Initial VLAN: 1
Authorization untagged VLAN: 100
Authorization tagged VLAN: N/A
Authorization ACL number/name: 3001
Authorization user profile: N/A
Termination action: Radius-request
Session timeout period: 2 s
Online from: 2013/03/02  13:14:15
Online duration: 0h 2m 15s

User MAC address              : 0015-e9a6-7cfe
AP name                       : ap1
Radio ID                      : 1
SSID                          : wlan_dot1x_ssid
BSSID                         : 0015-e9a6-7cf0
User name                     : ias
Authentication domain         : 1
Initial VLAN                  : 1
Authorization VLAN    : 100
Authorization ACL number      : 3001
Authorization user profile    : N/A
Authorization URL             : N/A
Authorization CAR             :
  Average input rate          : 102400 bps
  Average output rate         : 102400 bps
Termination action            : Radius-request
Session timeout period        : 2 sec
Online from                   : 2014/06/02 13:14:15
Online duration               : 0h 2m 15s
```

表1-2 display mac-authentication connection 命令显示信息描述表

字段	描述
Total connections	在线MAC地址认证用户个数
User MAC address	用户的MAC地址
Access interface	用户的接入接口名称
AP name	AP的名称
Radio ID	Radio的ID
SSID	服务集标识符
BSSID	用户所属的基本服务集标识符
Username	用户名
Authentication domain	认证时所用的ISP域的名称
Initial VLAN	初始的VLAN
Authorization untagged VLAN	授权的untagged VLAN
Authorization tagged VLAN	授权的tagged VLAN
Authorization VLAN	授权的VLAN
Authorization ACL number/name	（暂不支持）授权ACL的编号或名称。若未授权ACL，则显示为N/A
Authorization user profile	（暂不支持）授权用户的User profile名称
Authorization CAR	当服务器未授权用户CAR属性时，该字段显示为N/A。 当服务器授权用户CAR属性，将分为以下两个字段： • Average input rate ：上行平均速率，单位为 bps • Average output rate：下行平均速率，单位为 bps
Authorization URL	授权用户的重定向URL
Termination action	服务器下发的终止动作类型： • Default：会话超时时间到达后，强制用户下线 • Radius-Request：会话超时时间到达后，请求 MAC 地址认证用户进行重认证 用户采用本地认证时，该字段显示为N/A
Session timeout period	服务器下发的会话超时时间，该时间到达之后，用户所在的会话将会被删除，之后，对该用户所采取的动作，由Termination action字段的取值决定 用户采用本地认证时，该字段显示为N/A
Online from	MAC认证用户的上线时间
Online duration	MAC认证用户的在线时长

1.1.3 mac-authentication

mac-authentication 命令用来开启端口上或全局的 MAC 地址认证。

undo mac-authentication 命令用来关闭端口上或全局的 MAC 地址认证。

【命令】

mac-authentication

undo mac-authentication

【缺省情况】

所有端口及全局的 MAC 地址认证都处于关闭状态。

【视图】

系统视图

二层以太网接口视图

【缺省用户角色】

network-admin

【使用指导】

只有全局和端口的 MAC 地址认证均开启后，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。

```
<Sysname> system-view
[Sysname] mac-authentication
```

开启端口 GigabitEthernet1/0/1 上的 MAC 地址认证。

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

【相关命令】

- **display mac-authentication**

1.1.4 mac-authentication domain

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。

【命令】

mac-authentication domain *domain-name*

undo mac-authentication domain

【缺省情况】

未指定 MAC 地址认证用户使用的认证域时，使用系统缺省的认证域。缺省认证域的介绍请参见“用户接入与认证命令参考/AAA”中的命令 **domain default enable**。

【视图】

系统视图

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

domain-name：ISP 域名，为 1～255 个字符的字符串，不区分大小写。

【使用指导】

不同视图下指定的认证域的生效范围不同：

- 系统视图下指定的认证域对所有开启了 MAC 地址认证的端口生效。
- 二层以太网接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。

【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
```

【相关命令】

- **display mac-authentication**
- **domain default enable**（用户接入与认证命令参考/AAA）

1.1.5 mac-authentication guest-vlan

mac-authentication guest-vlan 命令用来配置端口的 MAC 地址认证的 Guest VLAN。

undo mac-authentication guest-vlan 命令用来恢复缺省情况。

【命令】

mac-authentication guest-vlan *guest-vlan-id*

undo mac-authentication guest-vlan

【缺省情况】

端口上未配置 MAC 地址认证的 Guest VLAN。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【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。

【使用指导】

配置此功能后，当 MAC 地址认证失败的情况下，用户可以继续被授权访问的 Guest VLAN 内的资源。

禁止删除已被配置为 Guest VLAN 的 VLAN，若要删除该 VLAN，请先通过 **undo mac-authentication guest-vlan** 命令取消 MAC 地址认证的 Guest VLAN 配置。

【举例】

配置端口 GigabitEthernet1/0/1 的 Guest VLAN 为 VLAN 100。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication guest-vlan 100
```

【相关命令】

- **display mac-authentication**
- **reset mac-authentication guest-vlan**

1.1.6 mac-authentication guest-vlan auth-period

mac-authentication guest-vlan auth-period 命令用来配置设备对 Guest VLAN 中的用户进行重新认证的时间间隔。

undo mac-authentication guest-vlan auth-period 命令用来恢复缺省情况。

【命令】

mac-authentication guest-vlan auth-period *period-value*

undo mac-authentication guest-vlan auth-period

【缺省情况】

设备对 Guest VLAN 中的用户进行重新认证的时间间隔为 30 秒。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

period-value：表示设备重新发起认证的时间间隔，取值范围为 1～3600，单位为秒。

【使用指导】

在 MAC 地址认证中，如果接入用户的端口上配置了 Guest VLAN，则该端口上认证失败的用户会被加入此 Guest VLAN。用户被加入 Guest VLAN 之后，设备将以指定的时间间隔对该用户发起重新认证，直到该用户认证成功。

【举例】

在端口 GigabitEthernet1/0/1 上配置设备对 Guest VLAN 中的用户进行重新认证的时间间隔为 150 秒。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] mac-authentication guest-vlan auth-period 150
```

【相关命令】

- **display mac-authentication**
- **mac-authentication guest-vlan**

1.1.7 mac-authentication host-mode

mac-authentication host-mode multi-vlan 命令用来指定端口工作在 MAC 地址认证的多 VLAN 模式。

undo mac-authentication host-mode 命令用来恢复缺省情况。

【命令】

mac-authentication host-mode multi-vlan

undo mac-authentication host-mode

【缺省情况】

端口工作在 MAC 地址认证的单 VLAN 模式。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【使用指导】

端口工作在多 VLAN 模式下时，如果相同 MAC 地址的用户在属于不同 VLAN 的相同端口再次接入，设备将能够允许用户的流量在新的 VLAN 内通过，且允许该用户的报文无需重新认证而在多个 VLAN 中转发。

端口工作在单 VLAN 模式下时，在用户已上线，且没有被下发授权 VLAN 情况下，如果此用户在属于不同 VLAN 的相同端口再次接入，则设备将让原用户下线，使得该用户能够在新的 VLAN 内重新开始认证。如果已上线用户被下发了授权 VLAN，则此用户在属于不同 VLAN 的相同端口再次接入时不会被强制下线。

【举例】

配置端口 GigabitEthernet1/0/1 工作在 MAC 地址认证的多 VLAN 模式。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication host-mode multi-vlan
```

【相关命令】

- **display mac-authentication**

1.1.8 mac-authentication max-user

mac-authentication max-user 命令用来配置端口上最多允许同时接入的 MAC 地址认证用户数。

undo mac-authentication max-user 命令用来恢复缺省情况。

【命令】

mac-authentication max-user *max-number*

undo mac-authentication max-user

【缺省情况】

端口上最多允许同时接入的 MAC 地址认证用户数为 4294967295。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

max-number：端口允许同时接入的 MAC 地址认证用户数的最大值，取值范围为 1～4294967295。

【使用指导】

由于系统资源有限，如果当前端口上接入的用户过多，接入用户之间会发生资源的争用，因此适当地配置该值可以使属于当前端口的用户获得可靠的性能保障。当接入此端口的 MAC 地址认证用户数超过最大值后，新接入的用户将被拒绝。

【举例】

配置端口 GigabitEthernet1/0/1 最多允许同时接入 32 个 MAC 地址认证用户。

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

【相关命令】

- **display mac-authentication**

1.1.9 mac-authentication re-authenticate server-unreachable keep-online

mac-authentication re-authenticate server-unreachable keep-online 命令用来配置重认证服务器不可达时端口上的 MAC 地址认证用户保持在线状态。

undo mac-authentication re-authenticate server-unreachable 命令用来恢复缺省情况。

【命令】

mac-authentication re-authenticate server-unreachable keep-online

undo mac-authentication re-authenticate server-unreachable

【缺省情况】

端口上的 MAC 地址认证在线用户重认证时，若认证服务器不可达，则会被强制下线。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【使用指导】

配置此命令后，在对 MAC 地址认证用户重认证过程中，若设备发现认证服务器状态不可达，则保持 MAC 地址认证用户在线。

是否对 MAC 地址认证在线用户进行周期性重认证由认证服务器授权的属性所决定。认证服务器通过下发 RADIUS 属性（session-timeout、Terminal-Action）来指定用户会话超时时长以及会话中止的动作类型，它们共同决定了如何对用户进行重认证。

- 当会话中止的动作类型为要求用户进行重认证时，端口会在用户会话超时时长到达后对该用户进行重认证；
- 当会话中止的动作类型为要求用户下线时，端口会在用户会话超时时长到达强制该用户下线；
- 当认证服务器未下发用户会话超时时长时，设备不会对用户进行重认证。

【举例】

配置端口 GigabitEthernet1/0/1 上的 MAC 地址认证在线用户进行重认证时，若服务器不可达，则保持在线状态。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication re-authenticate server-unreachable
keep-online
```

【相关命令】

- **display mac-authentication**

1.1.10 mac-authentication timer

mac-authentication timer 命令用来配置 MAC 地址认证的定时器参数。

undo mac-authentication timer 命令用来恢复缺省情况。

【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** }

【缺省情况】

下线检测定时器的值为 300 秒，静默定时器的值为 60 秒，服务器超时定时器的值为 100 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【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，取值范围为 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，取值范围为 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。

【使用指导】

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**）：用来设置在线用户空闲超时的时间间隔。若设备在一个下线检测定时器间隔之内，没有收到某在线用户的报文，将切断该用户的连接，同时通知 RADIUS 服务器停止对其计费。
- 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，设备不对来自认证失败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，如果到服务器超时定时器超时时设备一直没有收到 RADIUS 服务器的应答，则设备将在相应的端口上禁止此用户访问网络。

【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
```

【相关命令】

- **display mac-authentication**

1.1.11 mac-authentication timer auth-delay

mac-authentication timer auth-delay 命令用来开启 MAC 地址认证延迟功能，并配置 MAC 地址认证的延时时间。

undo mac-authentication timer auth-delay 命令用来恢复缺省情况。

【命令】

mac-authentication timer auth-delay *time*

undo mac-authentication timer auth-delay

【缺省情况】

MAC 地址认证延迟功能处于关闭状态，如果用户报文触发 MAC 地址认证，认证将会立刻开始。

【视图】

以太网接口视图

【缺省用户角色】

network-admin

【参数】

time：延迟 MAC 地址认证的时间，取值范围为 1～180，单位为秒。

【使用指导】

端口同时开启了 MAC 地址认证和 802.1X 认证的情况下，某些组网环境中希望设备对用户报文先进行 802.1X 认证。例如，有些客户端在发送 802.1X 认证请求报文之前，就已经向设备发送了其它报文，比如 DHCP 报文，因而触发了并不期望的 MAC 地址认证。这种情况下，就可以开启端口的 MAC 地址认证延时功能。

开启端口的 MAC 地址认证延时功能之后，端口就不会在收到用户报文时立即触发 MAC 地址认证，而是在等待一定的延迟时间之后，再会对之前收到的用户报文进行 MAC 地址认证。在此认证延迟期间，端口对用户报文的其它认证过程并不受影响。

开启了 MAC 地址认证延迟功能的接口上不建议同时配置端口安全的模式为 **mac-else-userlogin-secure** 或 **mac-else-userlogin-secure-ext**，否则 MAC 地址认证延迟功能不生效。端口安全模式的具体配置请参见“用户接入与认证命令参考”中的“端口安全”。

【举例】

开启 MAC 地址延迟认证功能，并指定 MAC 地址认证的延时时间为 10 秒。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication timer auth-delay 10
```

【相关命令】

- **display mac-authentication**
- **port-security port-mode**（用户接入与认证命令参考/端口安全）

1.1.12 mac-authentication user-name-format

mac-authentication user-name-format 命令用来配置 MAC 地址认证用户的帐号格式。

undo mac-authentication user-name-format 命令用来恢复缺省情况。

【命令】

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

undo mac-authentication user-name-format

【缺省情况】

使用用户的 MAC 地址作为用户名和密码，其中字母为小写，且不带连字符“-”。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

fixed：表示采用固定用户名账号。

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，区分大小写，不能包括字符@，缺省为 mac。

password：指定固定用户名的密码。

cipher：以密文方式设置密码。

simple：以明文方式设置密码，该密码将以密文形式存储。

string：密码字符串，区分大小写。明文密码为 1～63 个字符的字符串，密文密码为 1～117 个字符的字符串。

mac-address：表示使用用户的 MAC 地址作为用户名和密码。

with-hyphen [**six-section** | **three-section**]：带连字符“-”的 MAC 地址格式，**six-section** 表示六段式 MAC 地址格式，例如 xx-xx-xx-xx-xx-xx 或 XX-XX-XX-XX-XX-XX；**three-section** 表示三段式 MAC 地址格式，例如 xxxx-xxxx-xxxx 或 XXXX-XXXX-XXXX。如果不指定任何参数，缺省采用六段式 MAC 地址格式。

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

lowercase：MAC 地址中的字母为小写。

uppercase：MAC 地址中的字母为大写。

【使用指导】

若指定用户的 MAC 地址为用户名，则用户密码也为用户的 MAC 地址。这种情况下，每一个 MAC 地址认证用户都使用唯一的用户名进行认证，安全性高，但要求认证服务器端配置多个 MAC 形式的用户帐户。

若指定一个固定的用户名，则表示不论用户的 MAC 地址为何值，所有用户均使用设备上指定的一个固定用户名和密码作为身份信息进行认证。由于同一个端口下可以有多个用户进行认证，因此这种情况下端口上的所有 MAC 地址认证用户均使用同一个固定用户名账号进行认证，服务器端仅需要配置一个用户帐户即可满足所有认证用户的认证需求，适用于接入客户端比较可信的网络环境。

【举例】

配置 MAC 地址认证的用户名为 abc，密码是明文 xyz。

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

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

```
<Sysname> system-view
[Sysname] mac-authentication user-name-format mac-address without-hyphen uppercase
```

【相关命令】

- **display mac-authentication**

1.1.13 reset mac-authentication guest-vlan

reset mac-authentication guest-vlan 命令用来清除 Guest VLAN 内的 MAC 地址认证用户。

【命令】

reset mac-authentication guest-vlan interface *interface-type interface-number* [**mac-address** *mac-address*]

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

interface *interface-type interface-number*：表示使指定端口上的用户退出 Guest VLAN。*interface-type interface-number* 为端口类型和端口编号。

mac-address *mac-address*：表示使指定 MAC 地址的用户退出 Guest VLAN。若不指定本参数，则表示使指定端口上的所有用户退出 Guest VLAN。

【举例】

在端口 GigabitEthernet1/0/1 上使得 MAC 地址为 1-1-1 的 MAC 地址认证用户退出 Guest VLAN。

```
<Sysname> reset mac-authentication guest-vlan interface gigabitethernet 1/0/1 mac-address
1-1-1
```

【相关命令】

- **display mac-authentication**
- **mac-authentication guest-vlan**

1.1.14 reset mac-authentication statistics

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

【命令】

reset mac-authentication statistics [**interface** *interface-type interface-number*]

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

interface *interface-type interface-number*：清除指定端口的 MAC 地址认证统计信息。*interface-type interface-number* 为端口类型和端口编号。如果不指定本参数，则清除所有端口上的 MAC 地址认证统计信息。

【使用指导】

如果不指定任何参数，则清除所有 MAC 地址认证统计信息。

【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
```

【相关命令】

- **display mac-authentication**