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

mdc-admin

mdc-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
   Username format        : MAC address in lowercase(xxxxxxxxxxxx)
           Username       : mac
           Password       : Not configured
   Offline detect period  : 300 s
   Quiet period           : 60 s
   Server timeout         : 100 s
   Reauth period          : 3600 s
   Authentication domain  : Not configured, use default domain
 Online MAC-auth wired users    : 1

 Silent MAC users:
```

```
        MAC address       VLAN ID  From port              Port index
        0001-0000-0001    100      XGE1/0/2               21

Ten-GigabitEthernet1/0/1  is link-up
  MAC authentication         : Enabled
  Carry User-IP              : Disabled
  Authentication domain      : Not configured
  Auth-delay timer           : Enabled
      Auth-delay period      : 60 s
  Periodic reauth            : Enabled
      Reauth period          : 120 s
  Re-auth server-unreachable : Logoff
  Guest VLAN                 : 100
  Guest VLAN auth-period     : 150 s
  Critical VLAN              : Not configured
  Critical voice VLAN        : Disabled
  Host mode                  : Multiple VLAN
  Offline detection          : Enabled
  Authentication order       : Parallel

  Max online users           : 256
  Authentication attempts    : successful 2, failed 3
  Current online users       : 1
        MAC address       Auth state
        0001-0000-0001    Unauthenticated
```

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
Username format	MAC地址认证使用的用户名格式，有以下两种情况： • 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“MAC address in lowercase(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 • 若采用固定用户名格式，则显示“Fixed account”
Username:	用户名 • 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 • 采用固定用户名格式时，该值为配置的用户名（缺省为 mac）
Password:	用户名的密码 • 采用 MAC 地址格式时，该值显示为“Not configured” • 采用固定用户名格式时，配置的值将显示为******

字段	描述
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
Reauth period	重认证定时器的值
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
Ten-GigabitEthernet1/0/1 is link-up	端口Ten-GigabitEthernet1/0/1的链路状态
MAC authentication	当前端口的MAC地址认证开启状态
Carry User-IP	MAC地址认证请求携带用户IP地址关闭状态
Authentication domain	端口上指定的MAC地址认证用户使用的认证域
Auth-delay timer	MAC地址认证延迟功能的开启状态
Auth-delay period	配置的认证延迟时间
Periodic reauth	端口上MAC地址重认证开启状态
Reauth period	端口上配置的MAC地址重认证时间间隔
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，取值包括如下： • 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
Guest VLAN	端口配置的Guest VLAN，如果没有配置，则显示Not configured
Guest VLAN auth-period	进入Guest VLAN后发起重认证的时间间隔
Critical VLAN	端口配置的Critical VLAN，如果没有配置，则显示Not configured
Critical voice VLAN	端口配置MAC地址认证的Critical Voice VLAN功能的开启状态，包括如下取值： • Enabled：打开 • Disabled：关闭
Host mode	相同MAC地址用户的工作模式

字段	描述
	• 如果配置的是多 VLAN 模式，则显示 Multiple VLAN • 如果配置的是单 VLAN 模式，则显示 Single VLAN
Offline detection	MAC地址认证用户下线检测的开启状态，取值包括如下： • Enabled：处于开启状态 • Disabled：处于关闭状态
Authentication order	MAC地址认证和802.1X认证并行处理 • Default：处于关闭状态 • Parallel：处于开启状态
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，包括以下两种： • Authenticated：认证成功 • Unauthenticated：认证失败

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】

（独立运行模式）

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

（IRF 模式）

display mac-authentication connection [**chassis** *chassis-number* **slot** *slot-number* | **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

mdc-admin

mdc-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。

slot *slot-number*：显示指定单板上的 MAC 地址认证用户信息。*slot-number* 表示单板所在的槽位号。若不指定本参数，则显示所有单板上的 MAC 地址认证用户信息。（独立运行模式）

chassis *chassis-number* **slot** *slot-number*：显示指定单板的 MAC 地址认证用户信息。*chassis-number* 表示设备在 IRF 中的成员编号或者 PEX 对应的虚拟框号，*slot-number* 表示单板或 PEX 所在的槽位号。若不指定本参数，则显示所有单板上的 MAC 地址认证用户信息。（IRF 模式）

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。

【举例】

显示所有 MAC 地址认证在线用户信息。（独立运行模式）

```
<Sysname> display mac-authentication connection
Slot ID: 0
User MAC address: 0015-e9a6-7cfe
Access interface: Ten-GigabitEthernet1/0/1
Username: ias
Authentication domain: h3c
Initial VLAN: 1
Authorization untagged VLAN: 100
Authorization tagged VLAN: N/A
Authorization ACL ID: 3001
Termination action: Radius-request
Session timeout period: 2 s
Online from: 2013/03/02  13:14:15
Online duration: 0h 2m 15s

Total connections: 1.
```

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

字段	描述
User MAC address	用户的MAC地址
Access interface	用户的接入接口名称
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

字段	描述
Authorization tagged VLAN	授权的tagged VLAN
Authorization ACL ID	授权ACL编号
Terminate 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Terminate 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
Total connections	在线MAC地址认证用户个数

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

以太网接口视图

【缺省用户角色】

network-admin

mdc-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 Ten-GigabitEthernet1/0/1 上的 MAC 地址认证。

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

【相关命令】

- **display mac-authentication**

1.1.4 mac-authentication carry user-ip

mac-authentication carry user-ip 命令用来配置 MAC 地址认证请求中携带用户 IP 地址。

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

【命令】

mac-authentication carry user-ip

undo mac-authentication carry user-ip

【缺省情况】

MAC 地址认证请求中不携带用户 IP 地址。

【视图】

以太网接口视图

【缺省用户角色】

network-admin

mdc-admin

【使用指导】

在终端用户采用静态 IP 地址方式接入的组网环境中，如果终端用户擅自修改自己的 IP 地址，则整个网络环境中可能会出现 IP 地址冲突等问题。

为了解决以上问题，管理员可以在接口上开启 MAC 地址认证请求中携带用户 IP 地址的功能，用户在进行 MAC 地址认证时，设备会把用户的 IP 地址上传到 iMC 服务器。然后 iMC 服务器会把认证用户的 IP 地址和 MAC 地址与服务器上已经存在的 IP 与 MAC 的绑定表项进行匹配，如果匹配成功，则该用户 MAC 地址认证成功；否则，MAC 地址认证失败。

H3C 的 iMC 服务器上 IP 与 MAC 地址信息绑定表项的生成方式如下：

- 如果在 iMC 服务器上创建用户时手工指定了用户的 IP 地址和 MAC 地址信息，则服务器使用手工指定的 IP 和 MAC 信息生成该用户的 IP 与 MAC 地址的绑定表项。
- 如果在 iMC 服务器上创建用户时未手工指定用户的 IP 地址和 MAC 地址信息，则服务器使用用户初次进行 MAC 地址认证时使用的 IP 地址和 MAC 地址生成该用户的 IP 与 MAC 地址的绑定表项。

此功能仅对采用静态 IP 地址方式接入的认证用户才有效。在采用 DHCP 方式获取 IP 地址的情况下，因为用户 MAC 地址认证成功之后才可以进行 IP 地址获取，所以用户在进行 MAC 地址认证时，设备无法上传用户的 IP 地址。

在开启了 MAC 地址认证的接口上，不建议同时配置 **mac-authentication carry user-ip** 和 **mac-authentication guest-vlan** 命令，因为当同时配置了以上两条命令之后，加入 Guest VLAN 的用户无法再次发起 MAC 地址认证，用户会一直停留在 Guest VALN 中。

【举例】

在端口 Ten-GigabitEthernet1/0/1 上配置 MAC 地址认证请求携带用户 IP 地址功能。

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] mac-authentication carry user-ip
```

【相关命令】

- **mac-authentication**

1.1.5 mac-authentication critical vlan

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

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

【命令】

mac-authentication critical vlan *critical-vlan-id*

undo mac-authentication critical vlan

【缺省情况】

端口上未配置 MAC 地址认证的 Critical VLAN。

【视图】

以太网接口视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

critical-vlan-id：端口上指定的 Critical 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 用户认证时对应的 ISP 域下所有认证服务器都不可达的情况下被授权访问 Critical VLAN 内的资源。

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 MAC 地址认证的 Critical VLAN；同样，如果某个 VLAN 被指定为某个端口的 MAC 地址认证的 Critical VLAN，则该 VLAN 不能被指定为 Super VLAN。

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

【举例】

配置端口 Ten-GigabitEthernet1/0/1 的 Critical VLAN 为 VLAN 100。

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

【相关命令】

- **display mac-authentication**

- **reset mac-authentication critical-vlan**

1.1.6 mac-authentication critical-voice-vlan

mac-authentication critical-voice-vlan 命令用来开启端口下 MAC 地址认证的 Critical Voice VLAN 功能。

undo mac-authentication critical-voice-vlan 命令用来关闭端口下 MAC 地址认证的 Critical Voice VLAN 功能。

【命令】

mac-authentication critical-voice-vlan

undo mac-authentication critical-voice-vlan

【缺省情况】

端口下 MAC 地址认证的 Critical Voice VLAN 功能处于关闭状态。

【视图】

以太网接口视图

【缺省用户角色】

network-admin

mdc-admin

【使用指导】

端口上开启 MAC 地址认证 Critical Voice VLAN 功能后，当语音用户进行 MAC 地址认证采用的 ISP 域中的所有认证服务器都不可达时，端口将被加入到此端口上的 Voice VLAN 中。端口上语音 VLAN 的配置命令请参见“二层技术-以太网交换命令参考”中的“VLAN”。

设备通过 LLDP（Link Layer Discovery Protocol，链路层发现协议）来判断用户是否为语音用户，因此为保证 MAC 地址认证 Critical Voice VLAN 功能可以正常工作，请在开启此功能之前务必确保全局和相应端口下均已开启 LLDP 功能。有关 LLDP 功能的配置命令介绍请参见“二层技术-以太网交换命令参考”中的“LLDP”。

【举例】

开启端口 Ten-GigabitEthernet1/0/1 下 MAC 地址认证 Critical Voice VLAN 功能。

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] mac-authentication critical-voice-vlan
```

【相关命令】

- **display mac-authentication**
- **lldp enable**（二层技术-以太网交换命令参考/LLDP）
- **lldp global enable**（二层技术-以太网交换命令参考/LLDP）
- **reset mac-authentication critical-voice-vlan**
- **voice-vlan enable**（二层技术-以太网交换命令参考/VLAN）

1.1.7 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“安全命令参考/AAA”中的命令 **domain default enable**。

【视图】

系统视图

以太网接口视图

【缺省用户角色】

network-admin

mdc-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。
- 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 Ten-GigabitEthernet1/0/1 上接入的 MAC 地址认证用户使用的认证域为 aabbcc。

```
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] mac-authentication domain aabbcc
```

【相关命令】

- **display mac-authentication**
- **domain default enable**（安全命令参考/AAA）

1.1.8 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】

以太网接口视图

【缺省用户角色】

network-admin

mdc-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。

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 MAC 地址认证的 Guest VLAN；同样，如果某个 VLAN 被指定为某个端口的 MAC 地址认证的 Guest VLAN，则该 VLAN 不能被指定为 Super VLAN。

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 Ten-GigabitEthernet1/0/1 的 Guest VLAN 为 VLAN 100。

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

【相关命令】

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

1.1.9 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】

以太网接口视图

【缺省用户角色】

network-admin

mdc-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。

【举例】

在端口 Ten-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 ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] mac-authentication guest-vlan auth-period 150
```

【相关命令】

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

1.1.10 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】

以太网接口视图

【缺省用户角色】

network-admin

mdc-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。

对于接入 IP 电话类用户的端口，指定端口工作在 MAC 地址认证的多 VLAN 模式，可避免 IP 电话终端的报文所携带的 VLAN tag 发生变化后，因用户流量需要重新认证带来语音报文传输质量受干扰的问题。

【举例】

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

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

【相关命令】

- **display mac-authentication**

1.1.11 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】

以太网接口视图

【缺省用户角色】

network-admin

mdc-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 Ten-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 ten-gigabitethernet 1/0/1
```

```
[Sysname-Ten-GigabitEthernet1/0/1] mac-authentication max-user 32
```

【相关命令】

- **display mac-authentication**

1.1.12 mac-authentication offline-detect enable

mac-authentication offline-detect enable 命令用来开启端口的 MAC 地址认证下线检测功能。

undo mac-authentication offline-detect enable 命令用来关闭端口的 MAC 地址认证下线检测功能。

【命令】

mac-authentication offline-detect enable

undo mac-authentication offline-detect enable

【缺省情况】

端口的 MAC 地址认证下线检测功能处于开启状态。

【视图】

以太网接口视图

【缺省用户角色】

network-admin

mdc-admin

【使用指导】

开启端口的 MAC 地址认证下线检测功能后，若设备在一个下线检测定时器间隔之内，未收到此端口下某在线用户的报文，则将切断该用户的连接，同时通知 RADIUS 服务器停止对此用户进行计费。

关闭端口的 MAC 地址认证下线检测功能后，设备将不会对在线用户的状态进行检测。

【举例】

关闭端口 Ten-GigabitEthernet1/0/1 上的 MAC 地址认证下线检测功能。

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] undo mac-authentication offline-detect enable
```

【相关命令】

- **mac-authentication timer**

1.1.13 mac-authentication parallel-with-dot1x

mac-authentication parallel-with-dot1x 命令用来配置端口 MAC 地址认证和 802.1X 认证并行处理功能。

undo mac-authentication parallel-with-dot1x 命令用来恢复缺省情况。

【命令】

mac-authentication parallel-with-dot1x

undo mac-authentication parallel-with-dot1x

【缺省情况】

端口在收到源 MAC 地址未知的报文触发认证时，按照 802.1X 认证完成后再进行 MAC 地址认证的顺序进行处理。

【视图】

以太网接口视图

【缺省用户角色】

network-admin

mdc-admin

【使用指导】

端口采用 802.1X 和 MAC 地址组合认证功能适用于如下情况：

- 端口上同时开启了 802.1X 和 MAC 地址认证功能，并配置了 802.1X 认证的端口的接入控制方式为 macbased。
- 开启了端口安全功能，并配置了端口安全模式为 userlogin-secure-or-mac 或 userlogin-secure-or-mac-ext。端口安全模式的具体配置请参见“安全命令参考”中的“端口安全”。

在端口采用 802.1X 认证和 MAC 地址组合认证的情况下，如果想要在端口加入到 802.1X Guest VLAN 之前进行 MAC 地址认证并下发授权 VLAN，请通过本命令开启端口 MAC 地址认证和 802.1X 认证并行处理功能，并配置端口延迟加入 802.1X Guest VLAN 功能。关于端口延迟加入 802.1X Guest VLAN 配置命令的详细介绍，请参见“安全命令参考”中的“802.1X”。

开启了 MAC 地址认证和 802.1X 认证并行处理功能后，不建议配置端口的 MAC 地址认证延迟功能。

【举例】

在端口 Ten-GigabitEthernet1/0/1 上开启 MAC 地址认证和 802.1X 认证并行处理功能。

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] mac-authentication parallel-with-dot1x
```

1.1.14 mac-authentication re-authenticate

mac-authentication re-authenticate 命令用来开启 MAC 地址周期性重认证功能。

undo mac-authentication re-authenticate 命令用来关闭 MAC 地址周期性重认证功能。

【命令】

mac-authentication re-authenticate

undo mac-authentication re-authenticate

【缺省情况】

MAC 地址周期性重认证功能处于关闭状态。

【视图】

以太网接口视图

【缺省用户角色】

network-admin

mdc-admin

【使用指导】

端口开启了 MAC 地址认证用户的周期性重认证功能后，设备会周期性对该端口上的 MAC 地址认证在线用户进行重认证，以检测用户连接状态的变化，更新服务器下发的授权属性（例如 ACL、VLAN 等）。

【举例】

在端口 GigabitEthernet1/0/1 上开启 MAC 地址重认证功能，并配置周期性重认证时间间隔为 1800 秒。

```
<Sysname> system-view
[Sysname] mac-authentication timer reauth-period 1800
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication re-authenticate
```

【相关命令】

- **display mac-authentication**
- **mac-authentication timer**

1.1.15 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】

以太网接口视图

【缺省用户角色】

network-admin

mdc-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 Ten-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 ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] mac-authentication re-authenticate server-unreachable keep-online
```

【相关命令】

- **display mac-authentication**

1.1.16 mac-authentication timer (system view)

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* | **reauth-period** *reauth-period-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，周期性重认证定时器的值为 3600 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

mdc-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 60～2147483647，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。

reauth-period *reauth-period-value*：表示周期性重认证定时器，其中 *reauth-period-value* 表示周期性重认证定时器的值，取值范围为 60～7200，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。开启 MAC 地址认证下线检测功能后，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。配置 **offline-detect** 时，需要将 MAC 地址老化时间配成相同时间，否则会导致用户异常下线。
- 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。
- 周期性重认证定时器（**reauth-period**）：端口下开启了 MAC 地址周期性重认证功能后，设备可以此间隔为周期对端口上的在线用户发起重认证。对于已在线的 MAC 地址认证用户，要等当前重认证周期结束并且认证通过后才会按新配置的周期进行后续的重认证。
- 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**

1.1.17 mac-authentication timer auth-delay (interface view)

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

undo mac-authentication timer 命令用来将端口上指定的 MAC 地址认证定时器恢复为缺省情况。

【命令】

mac-authentication timer { **auth-delay** *auth-delay-time* | **reauth-period** *reauth-period-value* }

undo mac-authentication timer { **auth-delay** | **reauth-period** }

【缺省情况】

端口上未配置 MAC 地址认证延迟定时器，表示 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；端口上未配置 MAC 地址周期性重认证定时器，端口使用系统视图下配置的 MAC 地址周期性重认证定时器的取值。

【视图】

以太网接口视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

auth-delay *auth-delay-time*：表示 MAC 地址认证延迟定时器。其中 *auth-delay-time* 表示 MAC 地址认证延迟定时器的值，取值范围为 1～180，单位为秒。

reauth-period *reauth-period-value*：表示 MAC 地址认证周期性重认证定时器。其中 *reauth-period-value* 表示周期性重认证定时器的值，取值范围为 60～7200，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“安全命令参考”中的“端口安全”。

对 MAC 地址认证用户进行重认证时，设备将按照如下由高到低的顺序为其选择重认证时间间隔：服务器下发的重认证时间间隔、接口视图下配置的周期性重认证定时器的值、系统视图下配置的周期性重认证定时器的值、设备缺省的周期性重认证定时器的值。

对于已在线的 MAC 地址认证用户，要等当前重认证周期结束并且认证通过后才会按新配置的周期进行后续的重认证。

【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 ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] mac-authentication timer auth-delay 10
```

【相关命令】

- **display mac-authentication**
- **port-security port-mode**（安全命令参考/端口安全）

1.1.18 mac-authentication user-name-format

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。

【命令】

mac-authentication user-name-format { **fixed** [**account** *name*] [**password** { **cipher** | **simple** } *string*] | **mac-address** [{ **with-hyphen** | **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

mdc-admin

【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，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：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。

【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
```

【相关命令】

- **display mac-authentication**

1.1.19 reset mac-authentication critical-vlan

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

【命令】

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

【视图】

用户视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

interface *interface-type interface-number*：表示使指定端口上的用户退出 Critical 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 Critical VLAN。若不指定本参数，则表示使指定端口上的所有用户退出 Critical VLAN。

【举例】

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

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

【相关命令】

- **display mac-authentication**
- **mac-authentication critical vlan**

1.1.20 reset mac-authentication critical-voice-vlan

reset mac-authentication critical-voice-vlan 命令用来清除 MAC 地址认证 Critical Voice VLAN 内的 MAC 地址认证用户。

【命令】

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

【视图】

用户视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

interface *interface-type interface-number*：表示使指定端口上的用户退出 MAC 地址认证的 Critical Voice VLAN，其中 *interface-type interface-number* 为端口类型和端口编号。

mac-address *mac-address*：表示清除指定 MAC 地址的用户退出 MAC 地址认证的 Critical Voice VLAN。若不指定本参数，则表示使指定端口上的所有用户退出 Critical Voice VLAN。

【举例】

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

```
<Sysname> reset mac-authentication critical-voice-vlan interface ten-gigabitethernet 1/0/1
mac-address 1-1-1
```

【相关命令】

- **display mac-authentication**
- **mac-authentication critical-voice-vlan**

1.1.21 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

mdc-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 Ten-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 ten-gigabitethernet 1/0/1
mac-address 1-1-1
```

【相关命令】

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

1.1.22 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

mdc-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，则清除所有接口上的 802.1X 统计信息。

【举例】

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

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

【相关命令】

- **display mac-authentication**