目 录

1 802.1X

说明

本节命令仅在 SAP 板工作在二层模式时支持。

1.1 802.1X配置命令

1.1.1 display dot1x

【命令】

display dot1x [**sessions** | **statistics**] [**interface** *interface-list*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

sessions：显示 802.1X 的会话连接信息。

statistics：显示 802.1X 的相关统计信息。

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。

|：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 dot1x 命令用来显示802.1X的相关信息，包括会话连接信息、相关统计信息或配置信息等。

需要注意的是，如果不指定参数 **sessions** 或者 **statistics**，则显示 802.1X 的所有信息，包括会话连接信息、相关统计信息和配置信息等。

相关配置可参考命令 **reset dot1x statistics**、**dot1x**、**dot1x retry**、**dot1x max-user**、**dot1x port-control**、**dot1x port-method** 和 **dot1x timer**。

【举例】

显示 802.1X 的所有信息。

```
<Sysname> display dot1x
Equipment 802.1X protocol is enabled
CHAP authentication is enabled
Proxy trap checker is disabled
Proxy logoff checker is disabled
EAD quick deploy is enabled

Configuration: Transmit Period     30 s,  Handshake Period       15 s
               Quiet Period        60 s,  Quiet Period Timer is disabled
               Supp Timeout        30 s,  Server Timeout         100 s
               Reauth Period     3600 s
               The maximal retransmitting times          3
EAD quick deploy configuration:
               URL: http://192.168.19.23
               Free IP: 192.168.19.0 255.255.255.0
               EAD timeout:    30m

The maximum 802.1X user resource number is 2048 per slot
Total current used 802.1X resource number is 1

GigabitEthernet3/0/1  is link-up
  802.1X protocol is enabled
  Proxy trap checker is   disabled
  Proxy logoff checker is disabled
  Handshake is disabled
  Handshake secure is disabled
  802.1X unicast-trigger is enabled
  Periodic reauthentication is disabled
  The port is an authenticator
  Authenticate Mode is Auto
  Port Control Type is Port-based
  802.1X Multicast-trigger is enabled
  Mandatory authentication domain: NOT configured
  Guest VLAN: 4
  Auth-fail VLAN: NOT configured
  Critical VLAN: 3
  Critical recovery-action: reinitialize
  Max number of on-line users is 1024

  EAPOL Packet: Tx 1087, Rx 986
  Sent EAP Request/Identity Packets : 943
       EAP Request/Challenge Packets: 60
       EAP Success Packets: 29, Fail Packets: 55
  Received EAPOL Start Packets : 60
           EAPOL LogOff Packets: 24
           EAP Response/Identity Packets : 724
```

```
            EAP Response/Challenge Packets: 54
            Error Packets: 0
1. Authenticated user : MAC address: 0015-e9a6-7cfe

  Controlled User(s) amount to 1
```

表1-1 display dot1x 命令显示信息描述表

字段	描述
Equipment 802.1X protocol is enabled	全局的802.1X特性已经开启
CHAP authentication is enabled	是否使能CHAP认证
Proxy trap checker is disabled	是否检测通过代理登录用户的接入 • disable 表示不检测； • enable 表示检测到用户使用代理后，发送 Trap 报文
Proxy logoff checker is disabled	是否检测通过代理登录用户的接入 • disable 表示不检测； • enable 表示检测到用户使用代理后，切断用户连接
EAD quick deploy is enabled	EAD快速部署功能使能状态
Transmit Period	发送间隔定时器的时长
Handshake Period	设备向客户端发送握手报文的时间间隔
Reauth Period	周期性重认证的时间间隔
Quiet Period	静默定时器的时长
Quiet Period Timer is disabled	静默定时器的开启状态
Supp Timeout	客户端认证超时定时器的时长
Server Timeout	认证服务器超时定时器的时长
The maximal retransmitting times	设备向接入用户发送认证请求报文的最大次数
EAD quick deploy configuration	EAD快速部署功能的具体配置
URL	用户IE访问重定向的URL
Free IP	用户可访问的免认证网段
EAD timeout	ACL老化定时器超时时间
The maximum 802.1X user resource number per slot	每板最大支持的接入用户数
Total current used 802.1X resource number	当前在线接入用户数
GigabitEthernet3/0/1 is link-up	端口GigabitEthernet3/0/1的链路状态
802.1X protocol is disabled	该端口是否使能802.1X协议
Proxy trap checker is disabled	该端口是否检测通过代理登录用户的接入 • disable 表示不检测； • enable 表示检测用户使用代理后，发送 Trap 报文

字段	描述
Proxy logoff checker is disabled	该端口是否检测通过代理登录用户的接入 • disable 表示不检测； • enable 表示检测用户使用代理后，切断用户连接
Handshake is disabled	握手功能的使能状态
Handshake secure is disabled	安全握手功能的使能状态
802.1X unicast-trigger is disabled	802.1X单播触发功能的使能状态
Periodic reauthentication is disabled	周期性重认证功能的使能状态
The port is an authenticator	该端口担当设备端作用
Authenticate Mode is Auto	端口接入控制的模式为auto
Port Control Type is Port-based	端口接入控制方式为Port-based，即基于端口对接入用户进行认证
802.1X Multicast-trigger is enabled	802.1X组播触发功能的使能状态
Mandatory authentication domain	端口接入用户的强制认证域
Guest VLAN	端口配置的Guest VLAN，未配置则显示NOT configured
Auth-fail VLAN	端口配置的Auth Fail VLAN，未配置则显示NOT configured
Critical VLAN	端口配置的Critical VLAN，未配置则显示NOT configured
Critical recovery-action	端口配置的服务器可达时端口的恢复动作，reinitialize表示触发用户进行802.1X认证 未配置则显示NOT configured
Max number of on-line users	本端口最多可容纳的接入用户数
EAPOL Packet	EAPOL报文数目：Tx表示发送的报文数目；Rx表示接受的报文数目
Sent EAP Request/Identity Packets	发送的EAP Request/Identity报文数
EAP Request/Challenge Packets	发送的EAP Request/Challenge报文数
EAP Success Packets	发送的EAP Success报文数
Fail Packets	发送的EAP Failure报文数
Received EAPOL Start Packets	接收的EAPOL Start报文数
EAPOL LogOff Packets	接收的EAPOL LogOff报文数
EAP Response/Identity Packets	接收的EAP Response/Identity报文数
EAP Response/Challenge Packets	接收的EAP Response/Challenge报文数
Error Packets	接收的错误报文数
Authenticated user	认证通过的用户
Controlled User(s) amount	该端口受控用户数目

1.1.2 dot1x

【命令】

在系统视图下：

dot1x [**interface** *interface-list*]

undo dot1x [**interface** *interface-list*]

在以太网接口视图下：

dot1x

undo dot1x

【视图】

系统视图/以太网接口视图

【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。如果不指定本参数，则表示开启全局的 802.1X 特性。

【描述】

dot1x 命令用来开启指定端口上或全局的 802.1X 特性。**undo dot1x** 命令用来关闭指定端口上或全局的 802.1X 特性。

缺省情况下，所有端口及全局的 802.1X 特性都处于关闭状态。

需要注意的是：

- 802.1X 特性启动前后，均可以使用配置命令来配置全局或端口的 802.1X 特性参数。如果在开启全局 802.1X 特性前没有配置全局或端口的其它 802.1X 特性参数，则这些参数在运行时均为缺省值。
- 只有同时开启全局和端口的 802.1X 特性后，802.1X 的配置才能在端口上生效。

相关配置可参考命令 **display dot1x**。

【举例】

开启以太网端口 GigabitEthernet3/0/1 和 GigabitGigabitEthernet3/0/5 到 GigabitEthernet3/0/7 上的 802.1X 特性。

```
<Sysname> system-view
[Sysname] dot1x interface gigabitethernet 3/0/1 gigabitethernet 3/0/5 to gigabitethernet 3/0/7
```

或者

```
<Sysname> system-view
[Sysname] interface gigabitethernet 3/0/1
```

```
[Sysname-GigabitEthernet3/0/1] dot1x
[Sysname-GigabitEthernet3/0/1] quit
[Sysname] interface gigabitethernet 3/0/5
[Sysname-GigabitEthernet3/0/5] dot1x
[Sysname-GigabitEthernet3/0/5] quit
[Sysname] interface gigabitethernet 3/0/6
[Sysname-GigabitEthernet3/0/6] dot1x
[Sysname-GigabitEthernet3/0/6] quit
[Sysname] interface gigabitethernet 3/0/7
[Sysname-GigabitEthernet3/0/7] dot1x
```

开启全局的 802.1X 特性。

```
<Sysname> system-view
[Sysname] dot1x
```

1.1.3 dot1x authentication-method

【命令】

dot1x authentication-method { **chap** | **eap** | **pap** }

undo dot1x authentication-method

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

chap：启用 EAP 终结方式，并支持与 RADIUS 服务器之间采用 CHAP 类型的认证方法。

eap：启用 EAP 中继方式，并支持客户端与 RADIUS 服务器之间所有类型的 EAP 认证方法。

pap：启用 EAP 终结方式，并支持与 RADIUS 服务器之间采用 PAP 类型的认证方法。

【描述】

dot1x authentication-method 命令用来配置 802.1X 系统的认证方法。**undo dot1x authentication-method** 命令用来恢复缺省情况。

缺省情况下，设备启用 EAP 终结方式，并采用 CHAP 认证方法。

(1) EAP 终结认证方式：设备将收到的客户端 EAP 报文中的用户认证信息重新封装在标准的 RADIUS 报文报文中，然后采用 PAP 或 CHAP 认证方法与 RADIUS 服务器完成认证交互。该认证方式的优点是，现有的 RADIUS 服务器基本均可支持 PAP 和 CHAP 认证，无需升级服务器，但设备处理较为复杂，且目前仅能支持 MD5-Challenge 类型的 EAP 认证以及 iNode 802.1X 客户端发起的“用户名+密码”方式的 EAP 认证。

- PAP（Password Authentication Protocol，密码验证协议）通过用户名和口令来对用户进行验证，其特点是在网络上以明文方式传送用户名和口令，仅适用于对网络安全要求相对较低的环境。目前，仅 H3C iNode 802.1X 客户端支持此认证方法。
- CHAP（Challenge Handshake Authentication Protocol，质询握手验证协议）采用客户端与服务器端交互挑战信息的方式来验证用户身份，其特点是在网络上以明文方式传送用户名，以密文方式传输口令。与 PAP 相比，CHAP 认证保密性较好，更为安全可靠。

(2) EAP 中继：设备将收到的客户端 EAP 报文直接封装到 RADIUS 报文的属性字段中，发送给 RADIUS 服务器完成认证。该认证方式的优点是，设备处理简单，且可支持多种类型的 EAP 认证方法，例如 MD5-Challenge、EAP-TLS、PEAP 等，但要求服务器端支持相应的 EAP 认证方法。

需要注意的是：

- 本地认证支持 PAP 和 CHAP。
- 采用 RADIUS 认证方法时，PAP、CHAP、EAP 认证功能的最终实现，需要 RADIUS 服务器支持相应的 PAP、CHAP、EAP 认证。
- 若采用 EAP 认证方式，则 RADIUS 方案下的 **user-name-format** 配置无效，**user-name-format** 的介绍请参见“安全命令参考”中的“AAA”。

相关配置可参考命令 **display dot1x**。

【举例】

启用 EAP 终结方式，并支持与 RADIUS 服务器之间采用 PAP 类型的认证方法。

```
<Sysname> system-view
[Sysname] dot1x authentication-method pap
```

1.1.4 dot1x auth-fail vlan

【命令】

dot1x auth-fail vlan *authfail-vlan-id*

undo dot1x auth-fail vlan

【视图】

以太网接口视图

【缺省级别】

2：系统级

【参数】

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

【描述】

dot1x auth-fail vlan 命令用来配置指定端口的 Auth-Fail VLAN，即认证失败的用户被授权访问的 VLAN。**undo dot1x auth-fail vlan** 命令用来恢复缺省情况。

缺省情况下，端口没有配置 Auth-Fail VLAN。

需要注意的是：

- 这里的认证失败是认证服务器因某种原因明确拒绝用户认证通过，比如用户密码错误，而不是认证超时或网络连接等原因造成的认证失败。
- 在接入控制方式为 **portbased** 的端口上配置的 Auth-Fail VLAN，只有 802.1X 组播触发功能开启的情况下才生效。Auth-Fail VLAN 生效后，若将端口的接入控制方式由 **portbased** 修改为 **macbased**，则端口会离开 Auth-Fail VLAN。
- 在接入控制方式为 **macbased** 的端口上配置的 Auth-Fail VLAN，只有 MAC VLAN 功能开启的情况下才生效。Auth-Fail VLAN 生效后，若将端口的接入控制方式由 **macbased** 修改为

portbased，则已建立的 Auth-Fail VLAN 表项会被删除。Auth-Fail VLAN 表项中记录了加入 Auth-Fail VLAN 的 MAC 地址与端口上使能的 MAC VLAN，可以通过 **display mac-vlan** 查看。

- 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 Auth-Fail VLAN；同样，如果某个 VLAN 被指定为某个端口的 Auth-Fail 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”。
- 禁止直接删除已被配置为 Auth-Fail VLAN 的 VLAN，若要删除该 VLAN，请先通过命令 **undo dot1x auth-fail vlan** 取消 802.1X 的 Auth-Fail VLAN 配置。
- 同一个端口上可同时配置 Auth-Fail VLAN 和 Guest VLAN。

相关配置可参考命令 **dot1x** 和 **dot1x port-method**。

【举例】

在接口 GigabitEthernet3/0/1 上配置 Auth-Fail VLAN 为 3。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 3/0/1
[Sysname-GigabitEthernet3/0/1] dot1x auth-fail vlan 3
```

1.1.5 dot1x critical vlan

【命令】

dot1x critical vlan *vlan-id*

undo dot1x critical vlan

【视图】

以太网接口视图

【缺省级别】

2：系统级

【参数】

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。

【描述】

dot1x critical vlan 命令用来配置指定端口的 Critical VLAN，即当用户认证时对应的 ISP 域下所有认证服务器都不可达的情况下端口加入的 VLAN。**undo dot1x critical vlan** 命令用来恢复缺省情况。

缺省情况下，端口没有配置 Critical VLAN。

需要注意的是：

- 认证服务器不可达是指，因网络故障等原因导致的，用于认证用户的 ISP 域所引用的所有服务器都不可达；
- 接入控制方式为 MAC-based 时，端口上必须先使能 MAC VLAN 功能，配置的 Critical VLAN 才生效；
- 接入控制方式由 MAC-based 切换到 Port-based 时，已经建立的基于 Critical VLAN 的 MAC VLAN 表项会被删除，位于其中的用户将返回到其所在的初始 VLAN 中。

- 接入控制方式由 Port-based 切换到 MAC-based 时，端口将离开 Critical VLAN 并返回到其所在的初始 VLAN 中。
- 如果某个 VLAN 被指定为 Super VLAN，则不能被指定为 Critical VLAN；反之，Critical vlan 也不能被指定为 Super VLAN；
- 已经配置为 Critical VLAN 的 VLAN 不允许删除。若要删除配置为 Critical VLAN 的 VLAN，必须先取消 802.1X 的 Critical VLAN 配置；
- 若端口已经位于 802.1X 的 Guest VLAN 或 Auth-Fail VLAN，则当所有认证服务器都不可达时，端口并不会离开当前的 VLAN 而加入 Critical VLAN；
- 若端口已经位于 MAC 地址认证的 Guest VLAN，则当所有认证服务器都不可达时，端口会离开当前的 VLAN 并加入 Critical VLAN。

相关配置可参考命令 **dot1x**、**dot1x port-method** 和 **dot1x critical recovery-action**。

【举例】

在接口 GigabitEthernet3/0/1 上配置 Critical VLAN 为 VLAN 3。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 3/0/1
[Sysname-GigabitEthernet3/0/1] dot1x critical vlan 3
```

1.1.6 dot1x critical recovery-action

【命令】

dot1x critical recovery-action reinitialize

undo dot1x critical recovery-action

【视图】

以太网接口视图

【缺省级别】

2：系统级

【参数】

reinitialize：表示端口离开 Critical VLAN，并开始主动对用户进行认证。

【描述】

dot1x critical recovery-action 命令用于配置端口的恢复动作，即设备检测到认证服务器恢复为可达状态后端口执行的动作。**undo dot1x critical recovery-action** 命令用于恢复缺省情况。

缺省情况下，设备检测到服务器恢复为可达状态后，端口仅仅离开 Critical VLAN，不会对用户主动进行认证。

需要注意的是：

- 此命令仅用于和端口上的 Critical VLAN 配合使用。
- 接入控制方式为 MAC-based 时，如果端口上配置了恢复动作，则当服务器恢复可达后，处于 Critical VLAN 的端口会主动向已加入 Critical VLAN 的 MAC 地址发送单播报文触发其进行 802.1X 认证。

- 接入控制方式为 Port-based 时，如果端口上配置了恢复动作，则当服务器恢复可达后，处于 Critical VLAN 的端口会主动向客户端发送组播报文，触发端口上的客户端进行 802.1X 认证。
- 若需要实现认证服务器状态检测的实时性，使得设备能够及时发现有服务器恢复为可达状态，可配置认证服务器状态的探测功能。该功能的相关配置请参见“安全命令参考”中的“AAA”。

【举例】

在接口 GigabitEthernet3/0/1 上配置服务器可达后端口的动作为端口离开 Critical VLAN，并开始对用户进行认证。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 3/0/1
[Sysname-GigabitEthernet3/0/1] dot1x critical recovery-action reinitialize
```

1.1.7 dot1x domain-delimiter

【命令】

dot1x domain-delimiter *string*

undo dot1x domain-delimiter

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

string：指定 802.1X 认证支持的域名分隔符，为 1～16 个字符的字符串，可包括字符@、\、/或三者的任意组合，且可重复，例如@/、@/\、\@/、//等。

【描述】

dot1x domain-delimiter 命令用来配置 802.1X 支持的域名分隔符。**undo dot1x domain-delimiter** 命令用来恢复缺省情况。

缺省情况下，802.1X 仅支持域名分隔符@。

目前，802.1X 支持的域名分隔符包括@、\和/，对应的用户名格式分别为 *username@domain-name*，*domain-name\username* 和 *username/domain-name*，其中 *username* 为纯用户名、*domain-name* 为域名。如果用户名中包含有多个域名分隔符字符，则仅将第一个出现的域名分隔符识别为实际使用的域名分隔符，其它域名分隔符字符都被认为是域名中的一部分，例如，用户输入的用户名为 123/22\@abc，则认为纯用户名为 123，域名分隔符为/，域名为 22\@abc。

需要注意的是：

- 系统默认支持分隔符@，但如果通过本命令指定的域名分隔符中未包含分隔符@，则 802.1X 仅会支持命令中指定的分隔符。
- 对于使用域名分隔符\或者/的 802.1X 在线用户，不能通过 **cut connection user-name** *user-name* 命令切断其连接，也不能通过 **display connection user-name** *user-name* 命令查看到其相关信息。例如，执行命令 **cut connection user-name aaa\bbb** 后，不能切断在线用户 aaa\bbb 的连接。关于命令 **display connection** 和 **cut connection** 的介绍请参见“安全命令参考”中的“AAA”。

【举例】

配置 802.1X 支持的域名分隔符为@、\和/。

```
<Sysname> system-view
[Sysname] dot1x domain-delimiter @\/
```

1.1.8 dot1x guest-vlan

【命令】

在系统视图下：

dot1x guest-vlan *guest-vlan-id* [**interface** *interface-list*]

undo dot1x guest-vlan [**interface** *interface-list*]

在接口视图下：

dot1x guest-vlan *guest-vlan-id*

undo dot1x guest-vlan

【视图】

系统视图/以太网接口视图

【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。

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。如果不指定本参数，则表示配置所有二层以太网端口的 Guest VLAN。

【描述】

dot1x guest-vlan 命令用来配置指定端口的 Guest VLAN，即用户在未认证的情况下可以访问的 VLAN 资源，该 VLAN 内通常放置一些用于用户下载客户端软件或其他升级程序的服务器。**undo dot1x guest-vlan** 命令用来取消指定端口的 Guest VLAN。

缺省情况下，端口没有配置 Guest VLAN。

目前，仅接入控制方式为 Port-based 的端口支持 Guest VLAN。

需要注意的是：

- 只有开启 802.1X 特性的情况下，Guest VLAN 才能生效。
- 只有 802.1X 组播触发功能开启的情况下，Guest VLAN 才能生效。
- 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”。

- 禁止删除已被配置为 Guest VLAN 的 VLAN，若要删除该 VLAN，请先通过命令 **undo dot1x guest-vlan** 取消 802.1X 的 Guest VLAN 配置。
- 同一个端口下可同时配置 Guest VLAN 和 Auth-Fail VLAN。

相关配置可参考命令 **dot1x**、**dot1x port-method**、**dot1x multicast-trigger**。

【举例】

配置端口 GigabitEthernet3/0/1 的 Guest VLAN 为已经创建的 VLAN 999。

```
<Sysname> system-view
[Sysname] dot1x guest-vlan 999 interface gigabitethernet 3/0/1
```

配置端口 GigabitEthernet3/0/2～GigabitEthernet3/0/5 的 Guest VLAN 为已经创建的 VLAN 10。

```
<Sysname> system-view
[Sysname] dot1x guest-vlan 10 interface gigabitethernet 3/0/2 to gigabitethernet 3/0/5
```

配置所有端口的 Guest VLAN 为已经创建的 VLAN 7。

```
<Sysname> system-view
[Sysname] dot1x guest-vlan 7
```

配置端口 GigabitEthernet3/0/7 的 Guest VLAN 为已经创建的 VLAN 3。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 3/0/7
[Sysname-GigabitEthernet3/0/7] dot1x guest-vlan 3
```

1.1.9 dot1x critical recovery-action

【命令】

dot1x critical recovery-action reinitialize

undo dot1x critical recovery-action

【视图】

以太网接口视图

【缺省级别】

2：系统级

【参数】

reinitialize：表示端口离开 Critical VLAN，并开始主动对用户进行认证。

【描述】

dot1x critical recovery-action 命令用于配置端口的恢复动作，即设备检测到认证服务器恢复为可达状态后端口执行的动作。**undo dot1x critical recovery-action** 命令用于恢复缺省情况。

缺省情况下，设备检测到服务器恢复为可达状态后，端口仅仅离开 Critical VLAN，不会对用户主动进行认证。

需要注意的是：

- 此命令仅用于和端口上的 Critical VLAN 配合使用。
- 接入控制方式为 MAC-based 时，如果端口上配置了恢复动作，则当服务器恢复可达后，处于 Critical VLAN 的端口会主动向已加入 Critical VLAN 的 MAC 地址发送单播报文触发其进行 802.1X 认证。

- 接入控制方式为 Port-based 时，如果端口上配置了恢复动作，则当服务器恢复可达后，处于 Critical VLAN 的端口会主动向客户端发送组播报文，触发端口上的客户端进行 802.1X 认证。
- 若需要实现认证服务器状态检测的实时性，使得设备能够及时发现有服务器恢复为可达状态，可配置认证服务器状态的探测功能。该功能的相关配置请参见“安全命令参考”中的“AAA”。

【举例】

在接口 GigabitEthernet3/0/1 上配置服务器可达后端口的动作为端口离开 Critical VLAN，并开始对用户进行认证。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 3/0/1
[Sysname-GigabitEthernet3/0/1] dot1x critical recovery-action reinitialize
```

1.1.10 dot1x handshake

【命令】

dot1x handshake

undo dot1x handshake

【视图】

以太网接口视图

【缺省级别】

2：系统级

【参数】

无

【描述】

dot1x handshake 命令用于开启在线用户握手功能，通过设备端定期向客户端发送握手报文来探测用户是否在线。**undo dot1x handshake** 命令用于关闭在线用户握手功能。

缺省情况下，在线用户握手功能处于开启状态。

需要注意的是：

- 802.1X 的代理检测功能依赖于在线用户握手功能。在配置代理检测功能之前，必须先开启在线用户握手功能。关闭在线用户握手功能之前，必须先关闭配置代理检测功能。
- 建议在线用户握手功能与 iNode 客户端配合使用，以保证该功能可以正常运行。

【举例】

开启在线用户握手功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 3/0/4
[Sysname-GigabitEthernet3/0/4] dot1x handshake
```

1.1.11 dot1x handshake secure

【命令】

dot1x handshake secure

undo dot1x handshake secure

【视图】

以太网接口视图

【缺省级别】

2：系统级

【参数】

无

【描述】

dot1x handshake secure 命令用于开启在线用户握手安全功能。**undo dot1x handshake secure** 命令用于关闭在线用户握手安全功能。

缺省情况下，在线用户握手安全功能处于关闭状态。

需要注意的是：

- 在线用户握手安全功能的实现依赖于在线用户握手功能。为使在线用户握手安全功能生效，请保证在线用户握手功能处于开启状态。
- 建议在线用户握手安全功能与 iNode 客户端以及 iMC 服务器配合使用，以保证该功能可以正常运行。

相关配置请参见命令 **dot1x handshake**。

【举例】

开启在线用户握手安全功能。

```
<Sysname> system-view
[Sysname] interface Gigabitethernet 3/0/4
[Sysname-GigabitEthernet3/0/4] dot1x handshake secure
```

1.1.12 dot1x mandatory-domain

【命令】

dot1x mandatory-domain *domain-name*

undo dot1x mandatory-domain

【视图】

以太网接口视图

【缺省级别】

2：系统级

【参数】

domain-name：ISP 认证域名，为 1～24 个字符的字符串，不分区大小写。

【描述】

dot1x mandatory-domain 命令用来配置接口上 802.1X 用户的强制认证域。**undo dot1x mandatory-domain** 命令用来删除该接口上 802.1X 用户的认证域。

缺省情况下，未定义强制认证域。

需要注意的是：

- 从指定接口上接入的 802.1X 用户将按照如下先后顺序选择认证域：接口上配置的强制 ISP 域-->用户名中指定的 ISP 域-->系统缺省的 ISP 域。
- 接口上配置了强制认证域之后，使用不携带任何参数的 **display connection** 命令显示该接口下的用户连接信息时，所显示的用户域名为用户登录时使用的认证域名。但是，若要通过 **display connection domain** *isp-name* 命令显示该类用户、或者通过 **cut connection domain** *isp-name* 命令切断该类用户连接时，必须指定强制认证域名。关于命令 **display connection** 的介绍请参见“安全命令参考”中的“AAA”。

相关配置可参考命令 **display dot1x**。

【举例】

在接口 GigabitEthernet3/0/1 上配置 802.1X 用户使用强制认证域 my-domain。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 3/0/1
[Sysname-GigabitEthernet3/0/1] dot1x mandatory-domain my-domain
```

802.1X 用户 usera 通过认证后，通过命令 **display connection** 可查看接口 GigabitEthernet3/0/1 上的用户连接信息，该命令的具体介绍请参见“安全命令参考”中的“AAA”。

```
[Sysname-GigabitEthernet3/0/1] display connection interface gigabitethernet 3/0/1

Index=68  ,Username=usera@my-domian
MAC=0015-e9a6-7cfe
IP=3.3.3.3
IPv6=N/A
 Total 1 connection(s) matched.
```

1.1.13 dot1x max-user

【命令】

在系统视图下：

dot1x max-user *user-number* [**interface** *interface-list*]

undo dot1x max-user [**interface** *interface-list*]

在以太网接口视图下：

dot1x max-user *user-number*

undo dot1x max-user

【视图】

系统视图/以太网接口视图

【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，取值范围和 1～1024。

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】

dot1x max-user 命令用来设置 802.1X 在指定端口上可容纳接入用户数量的最大值。**undo dot1x 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为 1024。

需要注意的是：

- 在系统视图下执行该命令可以作用于参数 *interface-list* 所指定的端口，如果不指定任何端口则将作用于所有端口。
- 在以太网接口视图下执行该命令时，不能指定参数 *interface-list*，只能作用于当前端口。

相关配置可参考命令 **display dot1x**。

【举例】

配置端口 GigabitEthernet3/0/1 上最多可容纳 32 个接入用户。

```
<Sysname> system-view
[Sysname] dot1x max-user 32 interface gigabitethernet 3/0/1
```

或者

```
<Sysname> system-view
[Sysname] interface gigabitethernet 3/0/1
[Sysname-GigabitEthernet3/0/1] dot1x max-user 32
```

配置端口 GigabitEthernet3/0/2～GigabitEthernet3/0/5 中的每个端口上最多可容纳 32 个接入用户。

```
<Sysname> system-view
[Sysname] dot1x max-user 32 interface gigabitethernet 3/0/2 to gigabitethernet 3/0/5
```

1.1.14 dot1x multicast-trigger

【命令】

dot1x multicast-trigger

undo dot1x multicast-trigger

【视图】

以太网接口视图

【缺省级别】

2：系统级

【参数】

无

【描述】

dot1x multicast-trigger 命令用来使能 802.1X 的组播触发功能，即周期性地向客户端发送组播触发报文。**undo dot1x multicast-trigger** 命令用来关闭 802.1X 的组播触发功能。

缺省情况下，802.1X 的组播触发功能处于开启状态。

相关配置可参考命令 **display dot1x**。

【举例】

在接口 GigabitEthernet3/0/1 上开启 802.1X 的组播触发功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 3/0/1
[Sysname-GigabitEthernet3/0/1] dot1x multicast-trigger
```

1.1.15 dot1x port-control

【命令】

在系统视图下：

dot1x port-control { **authorized-force** | **auto** | **unauthorized-force** } [**interface** *interface-list*]

undo dot1x port-control [**interface** *interface-list*]

在以太网接口视图下：

dot1x port-control { **authorized-force** | **auto** | **unauthorized-force** }

undo dot1x port-control

【视图】

系统视图/以太网接口视图

【缺省级别】

2：系统级

【参数】

authorized-force：强制授权。指示端口始终处于授权状态，允许用户不经认证授权即可访问网络资源。

auto：自动识别。指示端口初始状态为非授权状态，仅允许 EAPOL 报文收发，不允许用户访问网络资源；如果认证通过，则端口切换到授权状态，允许用户访问网络资源。这也是最常见的情况。

unauthorized-force：强制非授权。指示端口始终处于非授权状态，不允许用户访问网络资源。

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】

dot1x port-control 命令用来设置端口的授权状态。**undo dot1x port-control** 命令用来恢复缺省的端口授权状态。

缺省情况下，端口的授权状态为 **auto**。

需要注意的是：

- 在系统视图下执行该命令时，若指定了参数 *interface-list*，则作用于参数 *interface-list* 所指定的端口；若不指定任何端口，则作用于当前系统中的所有端口。
- 在以太网接口视图下执行该命令时，不能指定参数 *interface-list*，只能作用于当前端口。

相关配置可参考命令 **display dot1x**。

【举例】

指定端口 GigabitEthernet3/0/1 处于强制非授权状态。

```
<Sysname> system-view
[Sysname] dot1x port-control unauthorized-force interface gigabitethernet 3/0/1
```

或者

```
<Sysname> system-view
[Sysname] interface gigabitethernet 3/0/1
[Sysname-GigabitEthernet3/0/1] dot1x port-control unauthorized-force
```

指定端口 GigabitEthernet3/0/2～GigabitEthernet3/0/5 均处于强制非授权状态。

```
<Sysname> system-view
[Sysname] dot1x port-control unauthorized-force interface gigabitethernet 3/0/2 to
gigabitethernet 3/0/5
```

1.1.16 dot1x port-method

【命令】

在系统视图下：

dot1x port-method { **macbased** | **portbased** } [**interface** *interface-list*]

undo dot1x port-method [**interface** *interface-list*]

在以太网接口视图下：

dot1x port-method { **macbased** | **portbased** }

undo dot1x port-method

【视图】

系统视图/以太网接口视图

【缺省级别】

2：系统级

【参数】

macbased：表示基于 MAC 地址对接入用户进行认证，即该端口下的所有接入用户均需要单独认证，当某个用户下线时，也只有该用户无法使用网络。

portbased：表示基于端口对接入用户进行认证，即只要该端口下的第一个用户认证成功后，其他接入用户无须认证就可使用网络资源，但是当第一个用户下线后，其他用户也会被拒绝使用网络。

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】

dot1x port-method 命令用来配置 802.1X 在指定端口上进行接入控制的方式。**undo dot1x port-method** 命令用来恢复缺省的接入控制方式。

缺省情况下，接入控制方式为 **macbased**。

需要注意的是：

- 在系统视图下执行该命令时，若指定了参数 *interface-list*，则作用于 *interface-list* 参数所指定的端口；若不指定任何端口，则作用于当前系统中的所有端口。
- 在以太网接口视图下执行该命令时，不能指定参数 *interface-list*，只能作用于当前端口。

相关配置可参考命令 **display dot1x**。

【举例】

在端口 GigabitEthernet3/0/1 上配置对接入用户进行基于端口的 802.1X 认证。

```
<Sysname> system-view
[Sysname] dot1x port-method portbased interface gigabitethernet 3/0/1
```

或者

```
<Sysname> system-view
[Sysname] interface gigabitethernet 3/0/1
[Sysname-GigabitEthernet3/0/1] dot1x port-method portbased
```

配置端口 GigabitEthernet3/0/2～GigabitEthernet3/0/5 上对接入用户进行基于端口的 802.1X 认证。

```
<Sysname> system-view
[Sysname] dot1x port-method portbased interface gigabitethernet 3/0/2 to gigabitethernet
3/0/5
```

1.1.17 dot1x quiet-period

【命令】

dot1x quiet-period

undo dot1x quiet-period

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

无

【描述】

dot1x quiet-period 命令用来开启静默定时器功能。**undo dot1x quiet-period** 命令用来关闭静默定时器功能。

缺省情况下，静默定时器功能处于关闭状态。

当 802.1X 用户认证失败以后，设备需要静默一段时间（该时间由静默定时器设置）。在静默期间，设备对该用户不进行 802.1X 认证的相关处理。

相关配置可参考命令 **display dot1x** 和 **dot1x timer**。

【举例】

开启静默定时器。

```
<Sysname> system-view
[Sysname] dot1x quiet-period
```

1.1.18 dot1x re-authenticate

【命令】

dot1x re-authenticate

undo dot1x re-authenticate

【视图】

以太网接口视图

【缺省级别】

2：系统级

【参数】

无

【描述】

dot1x re-authenticate 命令用来开启周期性重认证功能。**undo dot1x re-authenticate** 命令用来关闭周期性重认证功能。

缺省情况下，周期性重认证功能处于关闭状态。

端口启动了 802.1X 的周期性重认证功能后，设备会根据周期性重认证定时器（**dot1x timer reauth-period**）设定的时间间隔定期启动对该端口在线 802.1X 用户的认证，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、QoS Profile）。

相关配置可参考命令 **dot1x timer reauth-period**。

【举例】

在接口 GigabitEthernet3/0/1 上开启 802.1X 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] dot1x timer reauth-period 1800
[Sysname] interface gigabitethernet 3/0/1
[Sysname-GigabitEthernet3/0/1] dot1x re-authenticate
```

1.1.19 dot1x retry

【命令】

dot1x retry *max-retry-value*

undo dot1x retry

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

max-retry-value：向接入用户发送认证请求报文的最大次数，取值范围为 1～10。

【描述】

dot1x retry 命令用来设置设备向接入用户发送认证请求报文的最大次数。**undo dot1x retry** 命令用来将该最大发送次数恢复为缺省情况。

缺省情况下，向接入用户发送认证请求报文的最大次数为 2。

如果设备向用户发送认证请求报文后，在规定的时间里（可通过命令 **dot1x timer tx-period** 或者 **dot1x timer supp-timeout** 设定）没有收到用户的响应，则设备将向用户重发该认证请求报文，若设备累计发送认证请求报文的次数达到配置的最大值后，仍然没有得到用户响应，则停止发送认证请求。

需要注意的是：

- 此命令参数 *max-retry-value* 取值为 1 时表示只允许向用户发送一次认证请求报文，如果没有收到响应，不再重复发送；取值为 2 时表示在首次向用户发送请求又没有收到响应后将重复发送 1 次；……依次类推。
- 本命令设置后将作用于所有端口。

相关配置可参考命令 **display dot1x**。

【举例】

配置设备最多向接入用户发送 9 次认证请求报文。

```
<Sysname> system-view
[Sysname] dot1x retry 9
```

1.1.20 dot1x supp-proxy-check

【命令】

在系统视图下：

dot1x supp-proxy-check { **logoff** | **trap** } [**interface** *interface-list*]

undo dot1x supp-proxy-check { **logoff** | **trap** } [**interface** *interface-list*]

在以太网接口视图下：

dot1x supp-proxy-check { **logoff** | **trap** }

undo dot1x supp-proxy-check { **logoff** | **trap** }

【视图】

系统视图/以太网接口视图

【缺省级别】

2：系统级

【参数】

logoff：检测到用户使用代理后，切断用户连接。

trap：检测到用户使用代理后，向网管系统发送 Trap 报文。

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。如果不指定本参数，则表示开启全局的用户检测及接入控制。

【描述】

dot1x supp-proxy-check 命令用来设置设备对通过代理登录的用户的检测及接入控制。**undo dot1x supp-proxy-check** 命令用来取消设备对通过代理登录的用户的检测及相关控制的设置。

缺省情况下，设备不对通过代理登录的用户进行检测及接入控制。

需要注意的是：

- 该功能的实现需要 iNode 客户端程序的配合。
- 必须同时开启全局和指定端口的代理用户检测与控制，此特性的配置才能在该端口上生效。

相关配置可参考命令 **display dot1x**。

【举例】

配置端口 GigabitEthernet3/0/1～GigabitEthernet3/0/8 检测到用户使用代理后，切断该用户的连接。

```
<Sysname> system-view
[Sysname] dot1x supp-proxy-check logoff
[Sysname] dot1x supp-proxy-check logoff interface gigabitethernet 3/0/1 to gigabitethernet 3/0/8
```

配置端口 GigabitEthernet3/0/9 检测到登录的用户使用代理后，设备发送 Trap 报文。

```
<Sysname> system-view
[Sysname] dot1x supp-proxy-check trap
[Sysname] dot1x supp-proxy-check trap interface gigabitethernet 3/0/9
```

或者

```
<Sysname> system-view
[Sysname] dot1x supp-proxy-check trap
[Sysname] interface gigabitethernet 3/0/9
[Sysname-GigabitEthernet3/0/9] dot1x supp-proxy-check trap
```

1.1.21 dot1x timer

【命令】

dot1x timer { **handshake-period** *handshake-period-value* | **quiet-period** *quiet-period-value* | **reauth-period** *reauth-period-value* | **server-timeout** *server-timeout-value* | **supp-timeout** *supp-timeout-value* | **tx-period** *tx-period-value* }

undo dot1x timer { **handshake-period** | **quiet-period** | **reauth-period** | **server-timeout** | **supp-timeout** | **tx-period** }

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

handshake-period-value：握手定时器的值，取值范围为 5～1024，单位为秒。

quiet-period-value：静默定时器的值，取值范围为 10～120，单位为秒。

reauth-period-value：周期性重认证定时器的值，取值范围为 60～7200，单位为秒。

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

supp-timeout-value：客户端认证超时定时器的值，取值范围为 1～120，单位为秒。

tx-period-value：用户名请求超时定时器的值，取值范围为 10～120，单位为秒。

【描述】

dot1x timer 命令用来配置 802.1X 的各项定时器参数。**undo dot1x timer** 命令用来将指定的定时器恢复为缺省情况。

缺省情况下，握手定时器的值为 15 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，认证服务器超时定时器的值为 100 秒，客户端认证超时定时器的值为 30 秒，用户名请求超时定时器的值为 30 秒。

802.1X 认证过程受以下定时器的控制：

- 握手定时器（**handshake-period**）：此定时器是在用户认证成功后启动的，设备端以此间隔为周期发送握手请求报文，以定期检测用户的在线情况。如果配置发送次数为 N，则当设备端连续 N 次没有收到客户端的响应报文，就认为用户已经下线。
- 静默定时器（**quiet-period**）：对用户认证失败以后，设备端需要静默一段时间（该时间由静默定时器设置），在静默期间，设备端不处理该用户的认证功能。
- 周期性重认证定时器（**reauth-period**）：端口下开启了周期性重认证功能（通过命令 **dot1x re-authenticate**）后，设备端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 802.1X 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。
- 认证服务器超时定时器（**server-timeout**）：当设备端向认证服务器发送了 RADIUS Access-Request 请求报文后，设备端启动 **server-timeout** 定时器，若在该定时器设置的时长内，设备端没有收到认证服务器的响应，设备端将重发认证请求报文。
- 客户端认证超时定时器（**supp-timeout**）：当设备端向客户端发送了 EAP-Request/MD5 Challenge 请求报文后，设备端启动此定时器，若在该定时器设置的时长内，设备端没有收到客户端的响应，设备端将重发该报文。
- 用户名请求超时定时器（**tx-period**）：当设备端向客户端发送 EAP-Request/Identity 请求报文后，设备端启动该定时器，若在该定时器设置的时长内，设备端没有收到客户端的响应，则设备端将重发认证请求报文。另外，为了兼容不主动发送 EAPOL-Start 连接请求报文的客户端，设备会定期组播 EAP-Request/Identity 请求报文来检测客户端。**tx-period** 定义了该组播报文的发送时间间隔。

需要注意的是，一般情况下，用户无需修改定时器的值，除非在一些特殊或恶劣的网络环境下，可以使用该命令调节交互进程。修改后的定时器值，可立即生效。

相关配置可参考命令 **display dot1x**。

【举例】

设置认证服务器的超时定时器时长为 150 秒。

```
<Sysname> system-view
[Sysname] dot1x timer server-timeout 150
```

1.1.22 dot1x unicast-trigger

【命令】

dot1x unicast-trigger

undo dot1x unicast-trigger

【视图】

以太网接口视图

【缺省级别】

2：系统级

【参数】

无

【描述】

dot1x unicast-trigger 命令用来开启端口上的 802.1X 的单播触发功能。**undo dot1x unicast-trigger** 命令用来关闭 802.1X 的单播触发功能。

缺省情况下，802.1X 的单播触发功能处于关闭状态。

本功能开启后，当端口收到源 MAC 未知的报文时，主动向该 MAC 地址发送单播认证报文来触发认证。若设备端在设置的客户端认证超时时间内（该时间由 **dot1x timer tx-period** 设置）没有收到客户端的响应，则重发该报文（重发次数由 **dot1x retry** 设置）。

相关配置可参考命令 **display dot1x**、**dot1x timer tx-period** 和 **dot1x retry**。

【举例】

在端口 GigabitEthernet3/0/1 上开启 802.1X 的单播触发功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 3/0/1
[Sysname-GigabitEthernet3/0/1] dot1x unicast-trigger
```

1.1.23 reset dot1x statistics

【命令】

reset dot1x statistics [**interface** *interface-list*]

【视图】

用户视图

【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】

reset dot1x statistics 命令用来清除 802.1X 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 802.1X 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 802.1X 统计信息。

相关配置可参考命令 **display dot1x**。

【举例】

清除端口 GigabitEthernet3/0/1 上的 802.1X 统计信息。

```
<Sysname> reset dot1x statistics interface gigabitethernet 3/0/1
```

2 EAD快速部署命令

说明

本节命令仅在 SAP 板工作在二层模式时支持。

2.1 EAD快速部署命令

2.1.1 dot1x free-ip

【命令】

dot1x free-ip *ip-address* { *mask-address* **|** *mask-length* }

undo dot1x free-ip { *ip-address* { *mask* | *mask-length* } | **all** }

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

ip-address：免认证网段 IP 地址。

mask：免认证网段 IP 地址的掩码。

mask-length：免认证网段 IP 地址的掩码长度。

all：所有免认证网段。

【描述】

dot1x free-ip 命令用来配置 Free IP，即用户在 802.1X 认证成功之前可访问的免认证网段。**undo dot1x free-ip** 命令用来删除配置的 Free IP。

缺省情况下，未定义 Free IP。

需要注意的是：

- Free IP 功能与全局使能 MAC 认证、端口安全功能互斥；
- Free IP 功能只在端口接入控制的模式为 **auto** 的情况下生效；
- Free IP 可配置多条。

相关配置可参考命令 **display dot1x**。

【举例】

配置终端用户在 802.1X 认证之前可访问的免认证网段为 192.168.0.0/24。

```
<Sysname> system-view
[Sysname] dot1x free-ip 192.168.0.0 24
```

2.1.2 dot1x timer ead-timeout

【命令】

dot1x timer ead-timeout *ead-timeout-value*

undo dot1x timer ead-timeout

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

ead-timeout-value：EAD 规则的老化时间，取值范围为 1～1440，单位为分钟。

【描述】

dot1x timer ead-timeout 命令用来配置 EAD 规则的老化时间。**undo dot1x timer ead-timeout** 命令用来恢复缺省配置。

缺省情况下，EAD 规则的老化时间为 30 分钟。

相关配置可参考命令 **display dot1x**。

【举例】

配置 EAD 规则的老化时间为 5 分钟。

```
<Sysname> system-view
[Sysname] dot1x timer ead-timeout 5
```

2.1.3 dot1x url

【命令】

dot1x url *url-string*

undo dot1x url

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

url-string：重定向 URL 地址，为 1～64 个字符的字符串，区分大小写，格式为“http://string”。

【描述】

dot1x url 命令用来配置用户 HTTP 访问的重定向 URL，即用户在 802.1X 认证成功之前，如果使用浏览器访问非 Free IP 网段的其它网络，设备会将用户访问的 URL 重定向到已配置的 HTTP 访问的重定向地址。**undo dot1x url** 命令用来删除用户 HTTP 访问的重定向 URL。

缺省情况下，未定义重定向 URL。

需要注意的是：

- 重定向的 URL 和 Free IP 必须在同一个网段内，否则无法访问指定的重定向 URL；
- 用户 HTTP 访问的重定向 URL 可多次配置，但仅最后配置的一条有效。

相关配置可参考命令 **display dot1x** 和 **dot1x free-ip**。

【举例】

配置用户 HTTP 访问的重定向 URL 为 http://192.168.0.1。

```
<Sysname> system-view
[Sysname] dot1x url http://192.168.0.1
```