目 录

1 802.1X Client

1.1 802.1X Client功能配置命令

1.1.1 display dot1x supplicant

display dot1x supplicant 命令用来显示 802.1X Client 认证信息。

【命令】

display dot1x supplicant [**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*：表示显示指定接口上的 802.1X Client 认证信息。*interface-type interface-number* 为接口类型和接口编号。如果不指定本参数，则表示显示所有接口上的 802.1X Client 认证信息。

【举例】

显示接口 GigabitEthernet1/0/1 下 802.1X Client 认证信息。

```
<Sysname> display dot1x supplicant interface gigabitethernet 1/0/1
GigabitEthernet1/0/1
  Username             : aaa
  EAP method           : PEAP-MSCHAPv2
  Dot1x supplicant     : Enabled
  Anonymous identifier : bbb
  SSL client policy    : policy_1
  FSM state            : Init
  EAPOL-Start packets  : 0
```

表1-1 display dot1x supplicant interface 命令显示信息描述表

字段	描述
Username	用户名
EAP method	认证类型，包括以下取值： • MD5 • PEAP-GTC • PEAP-MSCHAPv2 • TTLS-GTC • TTLS-MSCHAPv2

字段	描述
Dot1x supplicant	802.1X Client功能所处状态： • Enabled：开启状态 • Disabled：关闭状态
Anonymous identifier	匿名认证用户名
SSL client policy	802.1X Client引用的SSL客户端策略
FSM state	802.1X Client认证状态，包括以下取值： • Init：初始状态 • Connecting：正在连接状态 • Authenticating：正在认证状态 • Authenticated：认证成功状态 • Held：静默状态
EAPOL-Start packets	发送的EAPOL-Start报文个数

1.1.2 dot1x supplicant anonymous identify

dot1x supplicant anonymous identify 命令用来配置 802.1X Client 匿名认证用户名。

undo dot1x supplicant anonymous identify 命令用来恢复缺省情况。

【命令】

dot1x supplicant anonymous identify *identifier*

undo dot1x supplicant anonymous identify

【缺省情况】

不存在 802.1X Client 匿名认证用户名。

【视图】

以太网接口视图

【缺省用户角色】

network-admin

【参数】

identifier：表示 802.1X Client 匿名认证用户名，为 1～253 个字符的字符串，区分大小写。

【使用指导】

仅在采用 PEAP-MSCHAPv2、PEAP-GTC、TTLS-MSCHAPv2 和 TTLS-GTC 认证方法时，才需要配置匿名认证用户名。802.1X Client 在第一阶段的认证过程中，优先发送匿名认证用户名，而在第二阶段将在被加密的报文中发送配置的认证用户名。配置了 802.1X Client 匿名认证用户名可有效保护认证用户名不在第一阶段的认证过程中被泄露。如果设备上没有配置匿名认证用户名，则两个认证阶段均使用配置的认证用户名进行认证。

当 802.1X Client 采用的认证方法为 MD5-Challenge 时，配置的 802.1X Client 匿名认证用户名无效，设备仍将使用配置的认证用户名进行认证。

如果认证服务器厂商不支持匿名认证用户名，则不要配置匿名认证用户名。

【举例】

配置 802.1X Client 匿名认证用户名为 bbb。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x supplicant anonymous identify bbb
```

【相关命令】

- **display dot1x supplicant**
- **dot1x supplicant enable**
- **dot1x supplicant username**

1.1.3 dot1x supplicant eap-method

dot1x supplicant eap-method 命令用来配置 802.1X Client 采用的 EAP 认证方法。

undo dot1x supplicant eap-method 命令用来恢复缺省情况。

【命令】

dot1x supplicant eap-method { **md5** | **peap-gtc** | **peap-mschapv2** | **ttls-gtc** | **ttls-mschapv2** }

undo dot1x supplicant eap-method

【缺省情况】

802.1X Client 采用的 EAP 认证方法为 MD5-Challenge。

【视图】

以太网接口视图

【缺省用户角色】

network-admin

【参数】

md5：表示采用的认证方法为 MD5-Challenge。

peap-gtc：表示采用的认证方法为 PEAP-GTC。

peap-mschapv2：表示采用的认证方法为 PEAP-MSCHAPv2。

ttls-gtc：表示采用的认证方法为 TTLS-GTC。

ttls-mschapv2：表示采用的认证方法为 TTLS-MSCHAPv2。

【使用指导】

配置的 802.1X Client 认证方法必须和认证服务器端支持的 EAP 认证方法保持一致。

【举例】

配置 802.1X Client 采用的认证方法为 PEAP-GTC。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x supplicant eap-method peap-gtc
```

【相关命令】

- **display dot1x supplicant**
- **dot1x supplicant enable**

1.1.4 dot1x supplicant enable

dot1x supplicant enable 命令用来开启 802.1X Client 功能。

undo dot1x supplicant enable 命令用来关闭 802.1X Client 功能。

【命令】

dot1x supplicant enable

undo dot1x supplicant enable

【缺省情况】

802.1X Client 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

【使用指导】

开启 802.1X Client 功能前，请确保设备（Authenticator）上关于 802.1X 认证的配置已完成。

如果被认证设备为 AP，且该 AP 上有用户在线时，关闭 802.1X Client 功能会导致在线用户被强制下线。

【举例】

开启 802.1X Client 功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x supplicant enable
```

【相关命令】

- **display dot1x supplicant**

1.1.5 dot1x supplicant password

dot1x supplicant password 命令用来配置 802.1X Client 认证密码。

undo dot1x supplicant password 命令用来恢复缺省情况。

【命令】

dot1x supplicant password { **cipher** | **simple** } *string*

undo dot1x supplicant password

【缺省情况】

不存在 802.1X Client 认证密码。

【视图】

以太网接口视图

【缺省用户角色】

network-admin

【参数】

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 1～127 个字符的字符串，密文密码为 1～201 个字符的字符串。

【举例】

配置 802.1X Client 的明文认证密码为 123456。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x supplicant password simple 123456
```

【相关命令】

- **display dot1x supplicant**
- **dot1x supplicant enable**

1.1.6 dot1x supplicant ssl-client-policy

dot1x supplicant ssl-client-policy 命令用来指定 802.1X Client 引用的 SSL 客户端策略。

undo dot1x supplicant ssl-client-policy 命令用来恢复缺省情况。

【命令】

dot1x supplicant ssl-client-policy *policy-name*

undo dot1x supplicant ssl-client-policy *policy-name*

【缺省情况】

802.1X Client 引用系统缺省的 SSL 客户端策略。

【视图】

以太网接口视图

【缺省用户角色】

network-admin

【参数】

policy-name：SSL 客户端策略名，为 1～31 个字符的字符串，不区分大小写，且引用的 SSL 客户端策略必须已存在。

【使用指导】

当 802.1X Client 认证采用 PEAP-MSCHAPv2、PEAP-GTC、TTLS-MSCHAPv2 或 TTLS-GTC 时，被认证设备作为 SSL 客户端会在 802.1X Client 第一阶段认证过程中，与对端 SSL 服务器进行 SSL 协商。在第二阶段被认证设备使用 SSL 协商出来的结果对交互的认证报文进行加密传输。

在 SSL 协商过程中，802.1X Client 作为 SSL 客户端连接 SSL 服务器时，需要使用本命令来引用 SSL 客户端策略。SSL 客户端策略中配置了 SSL 客户端启动时使用的 SSL 参数，包括使用的 PKI 域、支持的加密套件和使用的 SSL 协议版本。有关 SSL 客户端策略的详细配置请参见“安全配置指导”中的“SSL”。

当 802.1X Client 认证采用 MD5-Challenge 认证方法时，认证过程不会引用 SSL 客户端策略。

【举例】

在接口 GigabitEthernet1/0/1 下指定 802.1X Client 引用的 SSL 客户端策略为 policy_1。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x supplicant ssl-client-policy policy_1
```

【相关命令】

- **display dot1x supplicant**
- **dot1x supplicant enable**
- **ssl client-policy**（安全命令参考/SSL）

1.1.7 dot1x supplicant username

dot1x supplicant username 命令用来配置 802.1X Client 认证用户名。

undo dot1x supplicant username 命令用来恢复缺省情况。

【命令】

dot1x supplicant username *username*

undo dot1x supplicant username

【缺省情况】

不存在 802.1X Client 认证用户名。

【视图】

以太网接口视图

【缺省用户角色】

network-admin

【参数】

username：表示 802.1X Client 认证用户名，为 1～253 个字符的字符串，区分大小写。

【使用指导】

802.1X Client 认证用户名可以携带域名，域名中可用的分隔符包括@、\、/和.，对应的用户名格式分别为 *username@domain-name*、*domain-name\username*、*username/domain-name* 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，则设备仅将最后一个出现的域名分隔符识别为实际使用的域名分隔符。

若要指定域名分隔符\，则必须在输入时使用转义操作符\，即输入\\。域名分隔符的使用方法同命令**dot1x domain-delimiter**，有关此命令的详细介绍请参见“用户接入与认证命令参考”中的“802.1X”。

【举例】

配置 802.1X Client 认证用户名为 aaa。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x supplicant username aaa
```

【相关命令】

- **display dot1x supplicant**
- **dot1x domain-delimiter**（用户接入与认证命令参考/802.1X）
- **dot1x supplicant enable**