

# 目 录

1 802.1X Client.....	1-1
1.1 802.1X Client功能配置命令.....	1-1
1.1.1 dot1x supplicant anonymous identify.....	1-1
1.1.2 dot1x supplicant eap-method.....	1-2
1.1.3 dot1x supplicant enable .....	1-2
1.1.4 dot1x supplicant password.....	1-3
1.1.5 dot1x supplicant username .....	1-4

# 1 802.1X Client

## 1.1 802.1X Client功能配置命令

### 1.1.1 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】

AP 预配置视图

#### 【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] wlan ap ap1
[Sysname-wlan-ap-ap1] provision
[Sysname-wlan-ap-ap1-prvs] dot1x supplicant anonymous identify bbb
```

#### 【相关命令】

- `dot1x supplicant enable`
- `dot1x supplicant username`

## 1.1.2 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】

AP 预配置视图

### 【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] wlan ap ap1  
[Sysname-wlan-ap-ap1] provision  
[Sysname-wlan-ap-ap1-prvs] dot1x supplicant eap-method peap-gtc
```

### 【相关命令】

- `dot1x supplicant enable`

## 1.1.3 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】

AP 预配置视图

### 【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] wlan ap ap1
[Sysname-wlan-ap-ap1] provision
[Sysname-wlan-ap-ap1-prvs] dot1x supplicant enable
```

## 1.1.4 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】

AP 预配置视图

### 【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] wlan ap ap1
[Sysname-wlan-ap-ap1] provision
[Sysname-wlan-ap-ap1-prvs] dot1x supplicant password simple 123456
```

#### 【相关命令】

- **dot1x supplicant enable**

### 1.1.5 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】

AP 预配置视图

#### 【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“安全命令参考”中的“802.1X”。

#### 【举例】

```
# 配置 802.1X Client 认证用户名为 aaa。
<Sysname> system-view
[Sysname] wlan ap ap1
[Sysname-wlan-ap-ap1] provision
[Sysname-wlan-ap-ap1-prvs] dot1x supplicant username aaa
```

#### 【相关命令】

- **dot1x domain-delimiter**（安全命令参考/802.1X）
- **dot1x supplicant enable**