目 录

1 802.1X Client ····· 1-1
1.1 802.1X Client功能简介 ····· 1-1
1.2 802.1X Client配置限制和指导 ····· 1-1
1.3 802.1X Client功能配置任务简介 ····· 1-1
1.4 开启 802.1X Client功能 ····· 1-1
1.5 配置 802.1X Client认证用户名和密码 ····· 1-2
1.6 配置 802.1X Client采用的EAP认证方法 ····· 1-2
1.7 配置 802.1X Client匿名认证用户名 ····· 1-3
1.8 配置 802.1X Client引用的SSL客户端策略 ····· 1-3
1.9 802.1X Client功能显示和维护 ····· 1-4
1.10 802.1X Client功能典型配置举例 ····· 1-4
1.10.1 802.1X Client功能基本组网配置举例 ····· 1-4

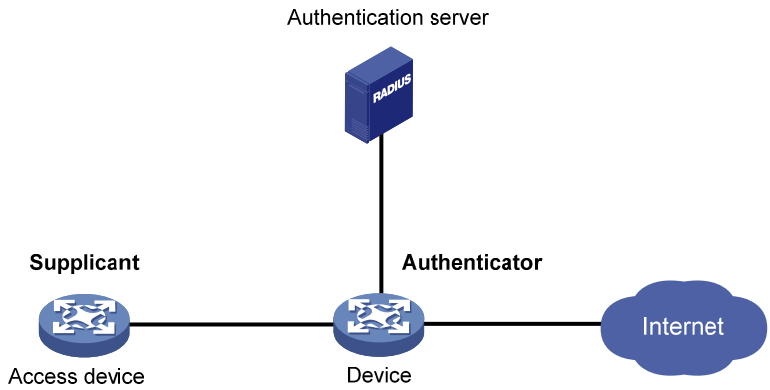
1 802.1X Client

1.1 802.1X Client功能简介

802.1X 的体系结构包括客户端、设备端和认证服务器。客户端通常有两种表现形式：安装了 802.1X 客户端软件的终端和网络设备。802.1X Client 功能允许网络设备作为客户端。有关 802.1X 体系的详细介绍请参见“用户接入与认证配置指导”中的“802.1X”。

应用了 802.1X Client功能的典型组网图如 图 1-1 所示：

图1-1 802.1X Client 组网图



1.2 802.1X Client配置限制和指导

关闭 802.1X Client 功能会导致已在线用户被强制下线，请谨慎操作。

1.3 802.1X Client功能配置任务简介

802.1X Client 功能配置任务如下：

(1) 开启 802.1X Client功能

(2) 配置 802.1X Client认证用户名和密码

(3) 配置 802.1X Client采用的EAP认证方法

(4) （可选）配置 802.1X Client匿名认证用户名

(5) 配置 802.1X Client引用的SSL客户端策略

当 802.1X Client 认证采用 PEAP-MSCHAPv2、PEAP-GTC、TTLS-MSCHAPv2 或 TTLS-GTC 认证方式时，需要引用 SSL 客户端策略。

1.4 开启802.1X Client功能

(1) 进入系统视图。

```
system-view
```

(2) 进入以太网接口视图。

interface *interface-type interface-number*

(3) 开启 802.1X Client 功能。

dot1x supplicant enable

缺省情况下，802.1X Client 功能处于关闭状态。

1.5 配置802.1X Client认证用户名和密码

1. 配置限制和指导

为确保认证成功，请将接入设备上配置的用户名和密码与认证服务器上配置的用户名和密码保持一致。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入以太网接口视图。

interface *interface-type interface-number*

(3) 配置 802.1X Client 认证用户名。

dot1x supplicant username *username*

(4) 配置 802.1X Client 认证密码。

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

1.6 配置802.1X Client采用的EAP认证方法

1. 802.1X Client支持的EAP认证方法

802.1X Client 支持的 EAP 认证方法分为 MD5-Challenge、PEAP-MSCHAPv2、PEAP-GTC、TTLS-MSCHAPv2 和 TTLS-GTC。

2. 配置限制和指导

若 802.1X Client 采用 MD5-Challenge 认证方法，则设备端（Authenticator）的 802.1X 认证方法可以配置为 PAP、CHAP 或 EAP.。

若 802.1X Client 采用其它认证方法，则设备端的认证方法必须配置为 EAP。

有关设备端认证方法的详细介绍，请参见“用户接入与认证配置指导”中的“802.1X”。

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。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入以太网接口视图。

interface *interface-type interface-number*

(3) 配置 802.1X Client 认证方法。

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

缺省情况下，802.1X Client 采用的 EAP 认证方法为 MD5-Challenge。

1.7 配置802.1X Client匿名认证用户名

1. 功能简介

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 认证采用的认证方法为 MD5-Challenge 时，被认证设备不会使用配置的匿名认证用户名认证，而是使用配置的认证用户名进行认证。

2. 配置限制和指导

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。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入以太网接口视图。

interface *interface-type interface-number*

(3) 配置 802.1X Client 匿名认证用户名。

dot1x supplicant anonymous identify *identifier*

1.8 配置802.1X Client引用的SSL客户端策略

1. 功能简介

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”。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入以太网接口视图。

interface *interface-type interface-number*

(3) 配置 802.1X Client 引用的 SSL 客户端策略。

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

缺省情况下，802.1X Client 引用系统缺省的 SSL 客户端策略。

1.9 802.1X Client功能显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 802.1X Client 功能的运行情况，通过查看显示信息验证配置的效果。

表1-1 802.1X Client 功能显示和维护

操作	命令
显示802.1X Client功能的配置信息、运行情况和统计信息	**display dot1x supplicant** [**interface** *interface-type interface-number*]

1.10 802.1X Client功能典型配置举例

1.10.1 802.1X Client功能基本组网配置举例

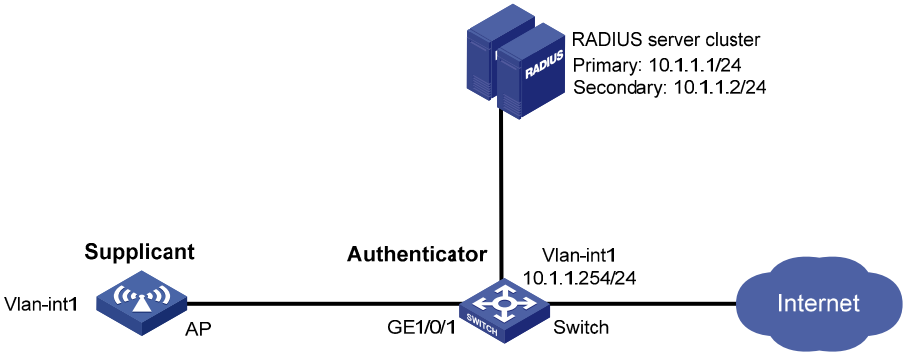
1. 组网需求

AP 通过交换机 Switch 的接口 GigabitEthernet1/0/1 接入网络，两台 RADIUS 服务器组成的服务器组与 Switch 相连，具体需求如下：

- AP 作为被认证设备，需要通过 Switch 上的 802.1X 认证才能接入网络。
- 主、备 RADIUS 服务器进行认证、授权，其 IP 地址分别为 10.1.1.1/24 和 10.1.1.2/24。
- Switch 作为 Authenticator 采用 EAP 中继认证方式与 RADIUS 服务器交互。
- Switch 开启 802.1X 认证。
- AP 属于 ISP 域 bbb。
- Switch 与 RADIUS 认证服务器交互报文时的共享密钥为 name。
- 802.1X Client 认证用户名为 aaa，密码为明文 123456。
- 802.1X Client 采用的 EAP 认证方法为 PEAP-MSCHAPv2。
- 对 AP 进行基于端口的 802.1X 认证。

2. 组网图

图1-2 802.1X Client 配置举例



3. 配置AP

(1) 配置各接口的 IP 地址（略）

(2) 配置 802.1X Client 功能

配置 802.1X Client 认证方法为 PEAP-MSCHAPv2。

```
<AP> system-view
[AP] interface gigabitethernet 1/0/1
[AP-GigabitEthernet1/0/1] undo shutdown
[AP-GigabitEthernet1/0/1] dot1x supplicant eap-method peap-mschapv2
```

配置 802.1X Client 认证用户名为 aaa，认证密码为明文 123456。

```
[AP-GigabitEthernet1/0/1] dot1x supplicant username aaa
[AP-GigabitEthernet1/0/1] dot1x supplicant password simple 123456
```

配置 802.1X Client 匿名认证用户名为 bbb。

```
[AP-GigabitEthernet1/0/1] dot1x supplicant anonymous identify bbb
```

开启 802.1X Client 功能。

```
[AP-GigabitEthernet1/0/1] dot1x supplicant enable
[AP-GigabitEthernet1/0/1] quit
```

4. 配置Switch

说明

- 下述配置步骤中包含了若干 RADIUS 协议的配置命令，关于这些命令的详细介绍请参见“用户接入与认证命令参考”中的“AAA”。
- 完成 RADIUS 服务器的配置，添加用户帐户，保证用户的认证/授权功能正常运行。

(1) 配置各接口的 IP 地址（略）

(2) 配置 RADIUS 方案

创建 RADIUS 方案 radius1 并进入其视图。

```
<Switch> system-view
[Switch] radius scheme radius1
```

配置主认证 RADIUS 服务器的 IP 地址。

```
[Switch-radius-radius1] primary authentication 10.1.1.1
```

配置备份认证 RADIUS 服务器的 IP 地址。

```
[Switch-radius-radius1] secondary authentication 10.1.1.2
```

配置 Switch 与认证 RADIUS 服务器交互报文时的共享密钥。

```
[Switch-radius-radius1] key authentication simple name
[Switch-radius-radius1] quit
```

说明

发送给服务器的用户名是否携带域名与服务器端是否接受携带域名的用户名以及服务器端的配置有关:

- 若服务器端不接受携带域名的用户名，或者服务器上配置的用户认证所使用的服务不携带域名后缀，则 Switch 上指定不携带用户名（without-domain）;
- 若服务器端可接受携带域名的用户名，且服务器上配置的用户认证所使用的服务携带域名后缀，则 Switch 上指定携带用户名（with-domain）。

(3) 配置 ISP 域

创建域 bbb 并进入其视图。

```
[Switch] domain bbb
```

配置 802.1X 用户使用 RADIUS 方案 radius1 进行认证、授权。

```
[Switch-isp-bbb] authentication lan-access radius-scheme radius1
[Switch-isp-bbb] authorization lan-access radius-scheme radius1
[Switch-isp-bbb] accounting lan-access none
[Switch-isp-bbb] quit
```

(4) 配置 802.1X

配置 802.1X 系统的认证方法为 EAP。

```
[Switch] dot1x authentication-method eap
```

配置对 AP 进行基于端口的 802.1X 认证。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] dot1x port-method portbased
```

指定接口上接入的 802.1X 用户使用强制认证域 bbb。

```
[Switch-GigabitEthernet1/0/1] dot1x mandatory-domain bbb
```

开启接口 GigabitEthernet1/0/1 的 802.1X。

```
[Switch-GigabitEthernet1/0/1] dot1x
[Switch-GigabitEthernet1/0/1] quit
```

开启全局 802.1X。

```
[Switch] dot1x
```

5. 验证配置

上述配置完成后，可通过 Switch 上输入 **display dot1x connection** 命令看到成功上线用户的信息。

```
[Switch] display dot1x connection
Total connections: 1
```

```
User MAC address: 70f9-6dd7-d1e0
Access interface: GigabitEthernet1/0/1
Username: aaa
Authentication domain: bbb
Authentication method: EAP
Initial VLAN: 1
Authorization untagged VLAN: N/A
Authorization tagged VLAN list: N/A
Authorization ACL ID: N/A
Authorization user profile: N/A
Termination action: N/A
Session timeout period: N/A
Online from: 2017/06/17 20:31:43
Online duration: 0h 1m 5s
```