目 录

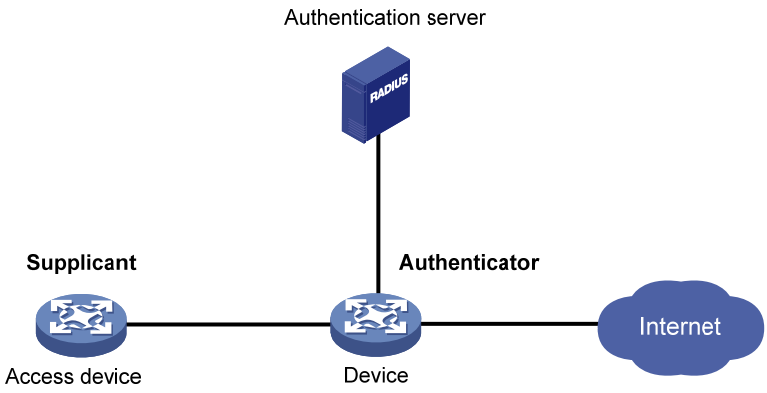
1 802.1X Client

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“安全配置指导”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功能配置任务简介

表1-1 802.1X Client 功能配置任务简介

配置任务	说明	详细配置
开启802.1X Client功能	必选	1.3.1
配置802.1X Client认证用户名和密码	必选	1.3.2
配置802.1X Client采用的EAP认证方法	必选	1.3.3
配置802.1X Client匿名认证用户名	可选	1.3.4

1.3 配置802.1X Client功能

1.3.1 开启 802.1X Client功能

注意

如果被认证 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。

开启 802.1X Client 功能前，请确保认证设备端上关于 802.1X 认证的配置已完成。有关 802.1X 认证的配置请参见“安全配置指导”中的“802.1X”。

表1-2 开启 802.1X Client 功能

操作	命令	说明
进入系统视图	**system-view**	-
创建手工AP，并进入AP视图	**wlan ap** *ap-name* [**model** *model-name*]	缺省情况下，未创建手工AP 创建AP时，需要输入型号名称
创建并进入AP provision视图	**provision**	缺省情况下，不存在provision视图
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

1.3.2 配置 802.1X Client认证用户名和密码

开启了 802.1X Client 功能的接入设备在进行 802.1X 认证时，会使用已配置的用户名和密码进行认证。

请确保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，否则会导致 802.1X 认证失败，最终造成被认证设备无法接入网络。

表1-3 配置 802.1X Client 认证用户名和密码

操作	命令	说明
进入系统视图	**system-view**	-
进入AP视图	**wlan ap** *ap-name* [**model** *model-name*]	-
进入AP provision视图	**provision**	-
配置802.1X Client认证用户名	**dot1x supplicant username** *username*	缺省情况下，不存在802.1X Client认证用户名
配置802.1X Client认证密码	**dot1x supplicant password** { **cipher** | **simple** } *password*	缺省情况下，不存在802.1X Client认证密码

1.3.3 配置 802.1X Client采用的EAP认证方法

802.1X Client 支持的 EAP 认证方法分为以下几种：

- MD5-Challenge（MD5-质询）
- PEAP-MSCHAPv2（Protected Extensible Authentication Protocol-Microsoft Challenge Handshake Authentication Protocol v2，受保护的扩展认证协议-Microsoft 质询握手身份验证协议版本 2）
- PEAP-GTC（Protected Extensible Authentication Protocol-Microsoft Generic Token Card，受保护的扩展认证协议-通用令牌卡）
- TTLS-MSCHAPv2（Tunneled Transport Layer Security-Microsoft Challenge Handshake Authentication Protocol v2，管道式传输层安全-Microsoft 质询握手身份验证协议版本 2）
- TTLS-GTC（Tunneled Transport Layer Security-Microsoft Generic Token Card，管道式传输层安全-通用令牌卡）

设备端（Authenticator）上支持两种 EAP 报文交互机制：EAP 中继和 EAP 终结。MD5-Challenge 认证方法支持以上两种 EAP 报文交互机制，而其余认证方法仅支持 EAP 中继。

说明

有关 EAP 报文交互机制的详细介绍，请参见“安全配置指导”中的“802.1X”。

需要注意的是，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。

表1-4 配置 802.1X Client 采用的 EAP 认证方法

操作	命令	说明
进入系统视图	**system-view**	-
进入AP视图	**wlan ap** *ap-name* [**model** *model-name*]	-
进入AP provision视图	**provision**	-
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

1.3.4 配置 802.1X Client匿名认证用户名

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。

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。

表1-5 配置 802.1X Client 匿名认证用户名

操作	命令	说明
进入系统视图	**system-view**	-
进入AP视图	**wlan ap** *ap-name* [**model** *model-name*]	-
进入AP provision视图	**provision**	-
配置802.1X Client匿名认证用户名	**dot1x supplicant anonymous identify** *identifier*	缺省情况下，不存在802.1X Client匿名认证用户名

1.4 802.1X Client功能典型配置举例

1.4.1 802.1X Client功能配置举例

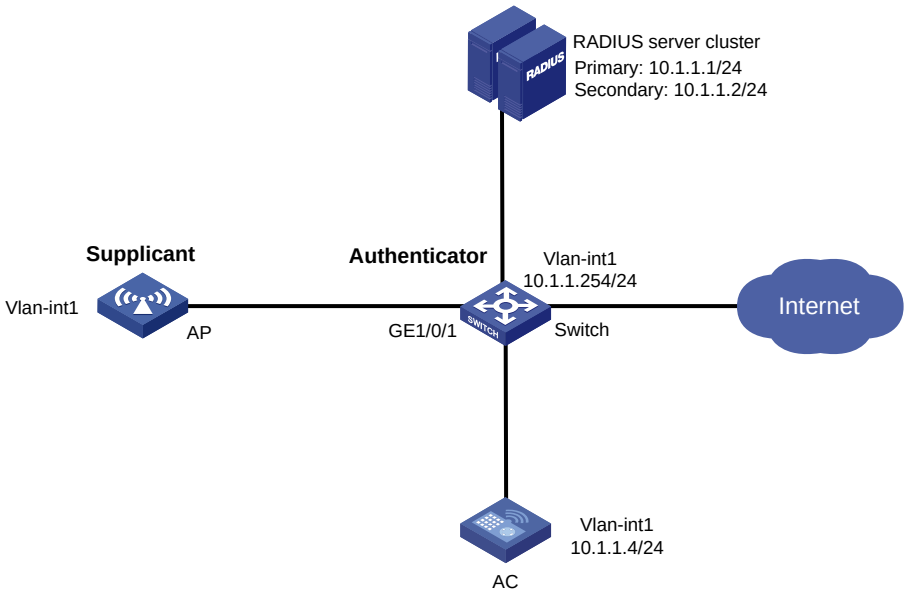
1. 组网需求

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 认证才能连接 AC。
- 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。
- AC 下发预配置到 AP，Switch 开启 802.1X Client 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. 配置步骤

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“安全命令参考”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 AC

- 配置各接口的 IP 地址（略）
- 配置 802.1X Client 功能

创建手工 AP，名称为 ap1，选择 AP 型号并配置序列号。

```
<AC> system-view
[AC] wlan ap ap1 model WA5320E-WiNet
[AC-wlan-ap-ap1] serial-id 219801A1FF8171E00361
```

创建并进入 AP provision 视图。

```
[AC-wlan-ap-ap1] provision
```

配置 802.1X Client 认证方法为 PEAP-MSCHAPv2。

```
[AC-wlan-ap-ap1-prvs] 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。

```
[AC-wlan-ap-ap1-prvs] dot1x supplicant username aaa
[AC-wlan-ap-ap1-prvs] dot1x supplicant password simple 123456
```

配置 802.1X Client 匿名认证用户名为 bbb。

```
[AC-wlan-ap-ap1-prvs] dot1x supplicant anonymous identify bbb
```

开启 802.1X Client 功能。

```
[AC-wlan-ap-ap1-prvs] dot1x supplicant enable
```

将预配置信息下发到 AP1。

```
[AC-wlan-ap-ap1-prvs] save wlan ap provision name ap1
[AC-wlan-ap-ap1-prvs] quit
[AC-wlan-ap-ap1] quit
```

(2) 配置 Switch

- 配置各接口的 IP 地址（略）
- 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
```

配置发送给 RADIUS 服务器的用户名不携带域名。

```
[Switch-radius-radius1] user-name-format without-domain
[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**）。

- 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
```

- 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
```
4. 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: 2015/06/16 19:10:32
Online duration: 0h 1m 1s
```