目 录

1 WLAN用户接入认证配置 ····· 1-1
1.1 WLAN用户接入认证简介 ····· 1-1
1.1.1 802.1X认证 ····· 1-1
1.1.2 MAC地址认证 ····· 1-4
1.1.3 入侵检测 ····· 1-6
1.1.4 认证模式 ····· 1-6
1.1.5 支持VLAN下发 ····· 1-6
1.1.6 支持授权ACL下发 ····· 1-7
1.1.7 支持User Profile下发 ····· 1-7
1.2 WLAN用户接入认证配置任务简介 ····· 1-8
1.3 配置准备 ····· 1-9
1.4 配置全局认证参数 ····· 1-9
1.4.1 配置OUI ····· 1-9
1.4.2 配置 802.1X支持的域名分隔符 ····· 1-9
1.4.3 配置 802.1X系统的认证方法 ····· 1-10
1.4.4 配置设备向接入用户发送认证请求报文最大次数 ····· 1-10
1.4.5 配置 802.1X定时器 ····· 1-11
1.4.6 配置MAC地址认证用户名及密码格式 ····· 1-12
1.4.7 配置MAC地址认证用户使用的ISP域 ····· 1-12
1.4.8 配置MAC地址认证定时器 ····· 1-12
1.5 配置WLAN用户认证接入认证参数 ····· 1-13
1.5.1 配置WLAN用户接入认证模式 ····· 1-13
1.5.2 配置 802.1X认证的EAP协议模式 ····· 1-13
1.5.3 配置忽略MAC地址认证结果 ····· 1-14
1.5.4 配置URL重定向功能 ····· 1-14
1.5.5 配置认证失败VLAN ····· 1-15
1.5.6 配置忽略授权信息 ····· 1-15
1.5.7 配置授权失败强制用户下线 ····· 1-16
1.5.8 配置入侵检测功能 ····· 1-16
1.5.9 配置 802.1X握手功能 ····· 1-17
1.5.10 配置 802.1X安全握手功能 ····· 1-17
1.5.11 配置 802.1X认证用户ISP域 ····· 1-18
1.5.12 配置 802.1X最大用户数 ····· 1-18

1.5.13 配置 802.1X重认证功能 ····· 1-18
1.5.14 配置MAC地址认证最大用户数 ····· 1-19
1.5.15 配置MAC地址认证用户ISP域 ····· 1-19
1.6 WLAN用户接入认证显示和维护 ····· 1-20
1.7 WLAN用户接入认证典型配置举例 ····· 1-20
1.7.1 802.1X认证（CHAP非加密本地认证）典型配置举例 ····· 1-20
1.7.2 802.1X认证（EAP-PEAP加密）典型配置举例 ····· 1-22
1.7.3 使用RADIUS服务器进行MAC地址认证典型配置举例 ····· 1-32

1 WLAN用户接入认证配置

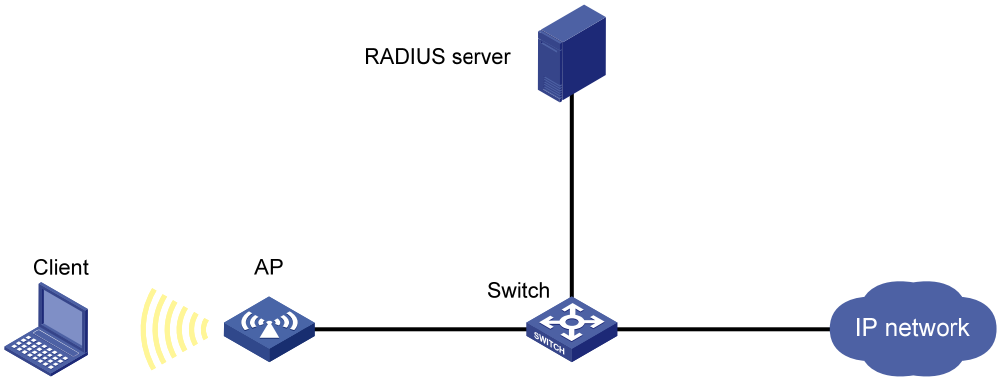
1.1 WLAN用户接入认证简介

WLAN 用户接入认证是一种基于用户的安全接入管理机制，根据用户 MAC 地址来进行访问控制。本特性主要实现 802.1X、MAC 地址认证和 OUI 认证三种认证方式。

- 802.1X 认证作为一种在无线网络中被广泛应用的接入控制机制，主要解决无线网络内认证和安全方面的问题。802.1X 认证系统使用 EAP（Extensible Authentication Protocol，可扩展认证协议）来实现客户端、设备端和认证服务器之间认证信息的交换。在客户端与设备端之间，EAP 协议报文使用 EAPOL（Extensible Authentication Protocol over LAN，局域网上的可扩展认证协议）封装格式的 802.11 报文，直接承载于无线环境中。在设备端与 RADIUS 服务器之间，可以使用两种方式来交换信息。一种是 EAP 协议报文由设备端进行中继，使用 RADIUS 协议封装 EAPOR 报文；另一种是 EAP 协议报文由设备端进行终结，采用包含 PAP 或 CHAP 属性的报文与 RADIUS 服务器进行认证交互。
- MAC 地址认证不需要用户安装任何客户端软件。设备在检测到用户的 MAC 地址以后，对该用户进行认证操作。认证过程中，不需要用户手动输入用户名或者密码，若该用户认证成功，则允许其访问网络资源，否则该用户则无法访问网络资源。
- OUI（Organizationally Unique Identifier，全球统一标识符）是 MAC 地址的前 24 位（二进制），是 IEEE 为不同设备供应商分配的一个全球唯一的标识符。采用 OUI 认证方式后，如果用户的 MAC 地址与设备配置的 OUI 能匹配上，则认证成功，否则认证失败。

FAT AP典型组网图如 图 1-1 所示。

图1-1 FAT AP 典型组网图



1.1.1 802.1X认证

说明

有关 802.1X 的体系结构、EAP 中继、EAP 终结及 EAP 报文的封装的详细介绍请参见“安全配置指导”中的“802.1X”。

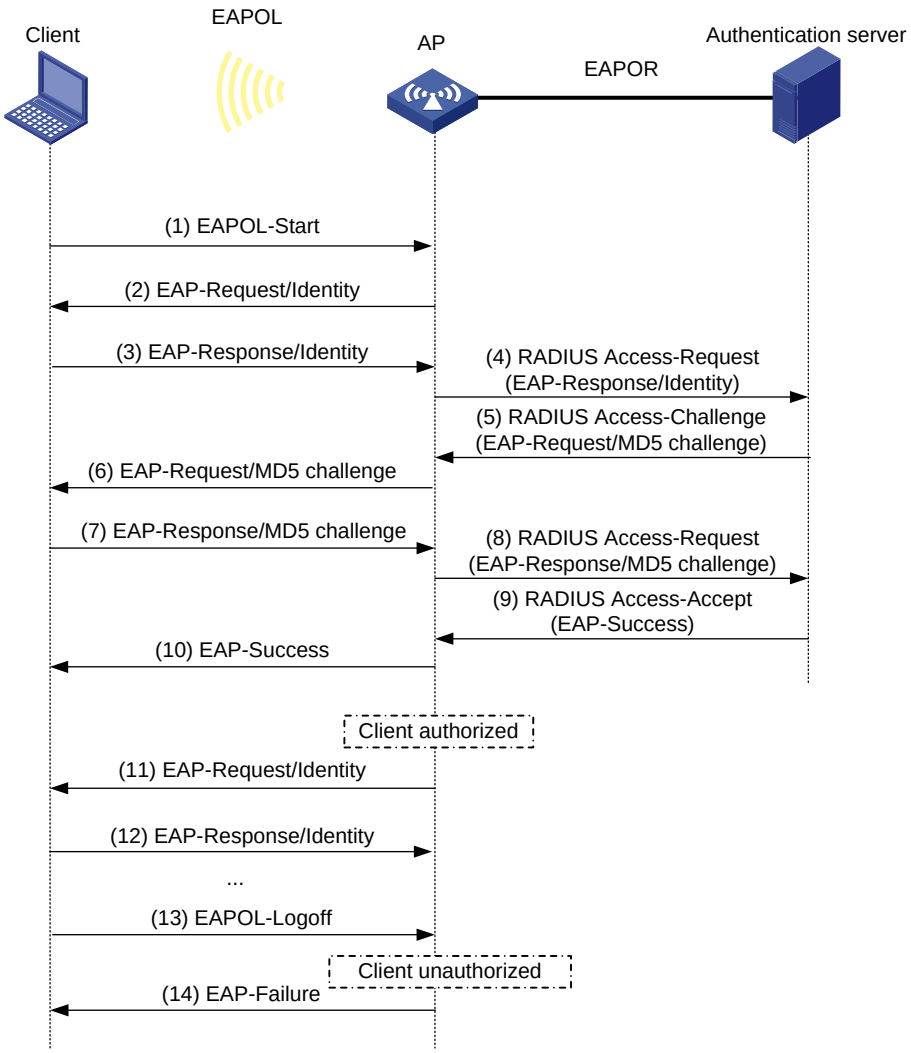
设备端支持采用 EAP 中继方式或 EAP 终结方式与远端 RADIUS 服务器交互。当无线组网方式为 FAT AP 时，则 FAT AP 为认证设备。

1. EAP中继认证方式

EAP 中继认证方式将 EAP 承载在其它高层协议中，如 EAP over RADIUS，以便 EAP 报文穿越复杂的网络到达认证服务器。一般来说，需要 RADIUS 服务器支持 EAP 属性：EAP-Message 和 Message-Authenticator。

如 图 1-2 所示，以MD5-Challenge类型的EAP认证为例，具体认证过程如下。

图1-2 EAP 中继方式流程



(1) 当用户需要访问外部网络时打开 802.1X 客户端程序，输入用户名和密码，发起连接请求。此时，客户端程序将向设备发出认证请求帧（EAPOL-Start），开始启动一次认证过程。有关客户端与 AP 建立连接的过程，请参见“WLAN 配置指导”中的“WLAN 安全”。

(2) 设备收到认证请求帧后，将发出一个 Identity 类型的请求帧（EAP-Request/Identity）要求客户端程序发送用户名。

(3) 客户端程序响应设备发出的请求，将用户名信息通过 Identity 类型的响应帧（EAP-Response/Identity）发送给设备。

(4) 设备将由客户端发送的响应帧中的 EAP 报文封装在 RADIUS 报文（RADIUS Access-Request）中，并发送给认证服务器进行处理。

(5) RADIUS 服务器收到设备转发的用户名信息后，将该信息与数据库中的用户名列表对比，找到该用户名对应的密码信息，用随机生成的一个 MD5 Challenge 对密码进行加密处理，同时将此 MD5 Challenge 通过 RADIUS Access-Challenge 报文发送给设备。

(6) 设备将 RADIUS 服务器发送的 MD5 Challenge 转发给客户端。

(7) 客户端收到由设备传来的 MD5 Challenge 后，用该 Challenge 对密码进行加密处理，生成 EAP-Response/MD5 Challenge 报文，并发送给设备。

(8) 设备将此 EAP-Response/MD5 Challenge 报文封装在 RADIUS 报文（RADIUS Access-Request）中发送给 RADIUS 服务器。

(9) RADIUS 服务器将收到的已加密的密码信息和本地经过加密运算后的密码信息进行对比，如果相同，则认为该用户为合法用户，并向设备发送认证通过报文（RADIUS Access-Accept）。

(10) 设备收到认证通过报文后向客户端发送认证成功帧（EAP-Success），允许用户访问网络。

(11) 用户在线期间，设备会通过向客户端定期发送握手报文的方法，对用户的在线情况进行监测。

(12) 客户端收到握手报文后，向设备发送应答报文，表示用户仍然在线。缺省情况下，若设备端发送的两次握手请求报文都未得到客户端应答，设备就会让用户下线，防止用户因为异常原因下线而设备无法感知。

(13) 客户端可以发送 EAPOL-Logoff 帧给设备，主动要求下线。

(14) 设备向客户端发送 EAP-Failure 报文。

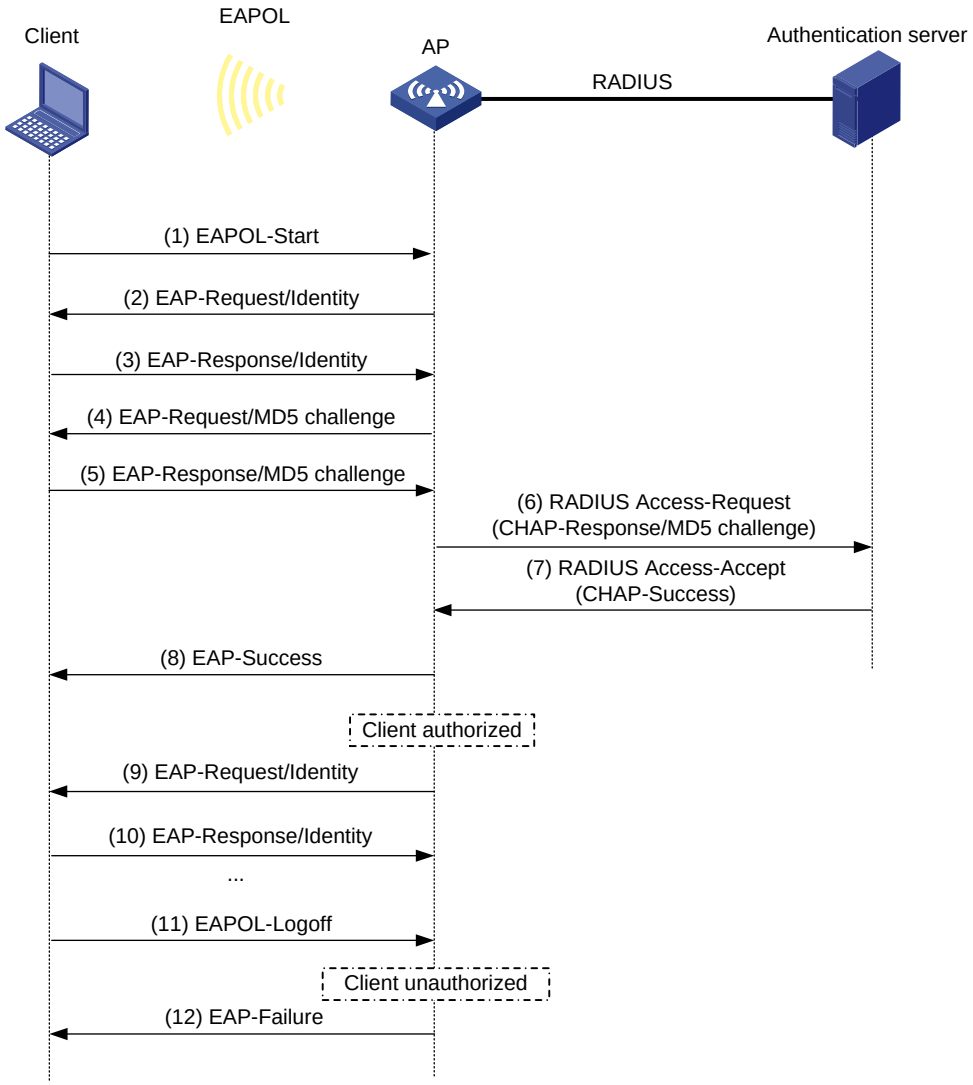
说明

EAP 中继方式下，需要保证在客户端和 RADIUS 服务器上选择一致的 EAP 认证方法，而在设备上，只需要通过 **dot1x authentication-method eap** 命令启动 EAP 中继方式即可。

2. EAP终结认证方式

这种方式将EAP报文在设备终结并映射到RADIUS报文中，利用标准RADIUS协议完成认证、授权和计费。设备与RADIUS服务器之间可以采用PAP或者CHAP认证方法。如 图 1-3 所示，以CHAP认证为例，具体的认证流程如下。

图1-3 FAT AP 802.1X 认证系统的 EAP 终结方式认证流程



EAP 终结方式与 EAP 中继方式的认证流程相比，不同之处在于对用户密码信息进行加密处理的 MD5 challenge 由认证设备生成的，之后认证设备会把用户名、MD5 challenge 和客户端加密后的密码信息一起发送给 RADIUS 服务器，进行相关的认证处理。

3. EAP报文的封装

有关 EAP 报文的封装的详细介绍，请参见“安全配置指导”中的“802.1X”。

4. 802.1X的认证触发方式

802.1X 认证触发方式有两种：当设备收到客户端关联回应报文后，客户端向设备发送 EAPOL-Start 报文触发认证；当设备收到客户端关联回应报文后，由设备主动向该客户端发送 Identity 类型的 EAP-Request 帧来触发认证，若设备端在设置的时长内没有收到客户端的响应，则重发该报文。

1.1.2 MAC地址认证

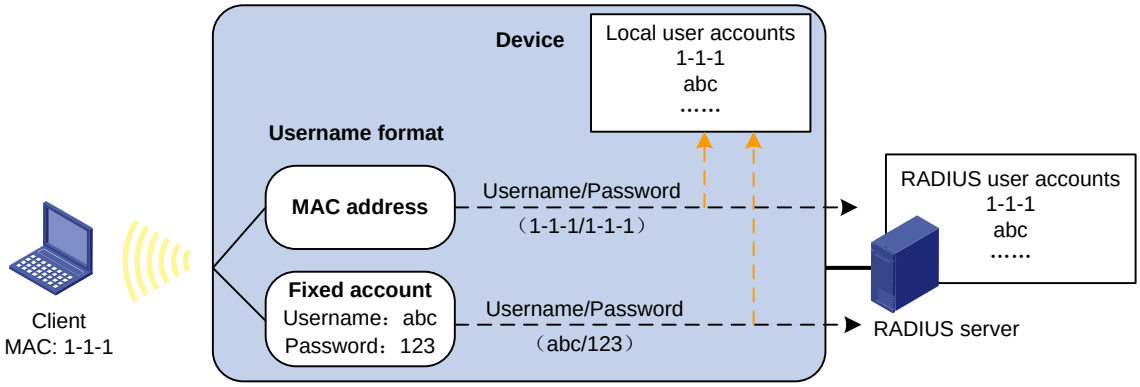
目前设备支持两种方式的 MAC 地址认证，通过 RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）服务器进行远程认证和在接入设备上进行本地认证。当无线组网

方式为 FAT AP 时，则 FAT AP 为认证设备。有关远程 RADIUS 认证和本地认证的详细介绍请参见“安全配置指导”中的“AAA”。

根据设备最终用于验证用户身份的用户名格式和内容的不同，可以将 MAC 地址认证使用的用户帐户格式分为两种类型：

- MAC 地址用户名密码：使用用户的 MAC 地址作为用户名和密码进行认证，即每个用户使用不同的用户名和密码进行认证。
- 固定用户名密码：设备上所有 MAC 地址认证用户均使用所配置的用户名和密码进行认证，即所有用户使用同一个用户名和密码进行认证。用户名为 1～55 个字符的字符串，区分大小写，不能包括字符‘@’。密码可以设置为明文或者密文，明文密码为 1～63 个字符的字符串，密文密码为 1～117 个字符的字符串。

图1-4 不同用户名格式下的 MAC 地址认证示意图



(1) RADIUS 服务器认证方式进行 MAC 地址认证

当选用 RADIUS 服务器认证方式进行 MAC 地址认证时，设备作为 RADIUS 客户端，与 RADIUS 服务器配合完成 MAC 地址认证操作：

- 若采用 MAC 地址用户名格式，则设备将检测到的用户 MAC 地址作为用户名和密码发送给 RADIUS 服务器进行验证。
- 若采用固定用户名格式，则设备将一个已经在本地指定的 MAC 地址认证用户使用的固定用户名和对应的密码作为待认证用户的用户名和密码，发送给 RADIUS 服务器进行验证。

RADIUS 服务器完成对该用户的认证后，认证通过的用户可以访问网络。

(2) 本地认证方式进行 MAC 地址认证

当选用本地认证方式进行 MAC 地址认证时，直接在设备上完成对用户的认证。需要在设备上配置本地用户名和密码：

- 若采用 MAC 地址用户名格式，则设备将检测到的用户 MAC 地址作为待认证用户的用户名和密码与配置的本地用户名和密码进行匹配。
- 若采用固定用户名格式，则设备将一个已经在本地指定的 MAC 地址认证用户使用的固定用户名和对应的密码作为待认证用户的用户名和密码与配置的本地用户名和密码进行匹配。

用户名和密码匹配成功后，用户可以访问网络。

1.1.3 入侵检测

当设备检测到一个未通过认证的用户试图访问网络时，如果开启入侵检测功能，设备将对其所在的BSS采取相应的安全策略。

入侵检测所采取的安全模式，包括以下几种：

- temporary-block：缺省模式。如果设备检测到未通过认证用户的关联请求报文，临时将该报文的源MAC地址加入阻塞MAC地址列表中，在一段时间内，源MAC地址为此非法MAC地址的无线客户端将不能和AP建立连接，在这段时间过后恢复正常。该MAC地址的阻塞时间由阻塞非法入侵用户时长决定。
- service-stop：直接关闭收到未通过认证用户的关联请求报文的BSS所提供的服务，直到用户在Radio口上重新生成该BSS。
- temporary-service-stop：关闭收到未通过认证用户的关联请求报文的BSS一段时间，该时间由临时关闭服务时长决定。

1.1.4 认证模式

WLAN用户接入认证支持以下几种认证模式：

表1-1 WLAN用户接入认证模式描述表

认证模式		工作机制	入侵检测
缺省情况	bypass	不对用户进行认证	无效
采用802.1X认证	dot1x	只进行802.1X认证	可触发
采用MAC地址认证	mac	只进行MAC地址认证	可触发
采用802.1X和MAC地址认证组合认证	mac-or-dot1x	先进行MAC地址认证，如果失败，再进行802.1X认证，如果认证成功，则不进行802.1X认证	可触发
	dot1x-or-mac	先进行802.1X认证，如果失败，再进行MAC地址认证，如果认证成功，则不进行MAC地址认证	
	oui-or-dot1x	先进行OUI认证，如果失败，再进行802.1X认证，如果认证成功，则不进行802.1X认证	

1.1.5 支持VLAN下发

1. 授权VLAN

用户通过802.1X或MAC地址认证方式认证成功后，授权服务器可以下发授权VLAN，用来限制用户访问网络资源。下发的授权VLAN信息可以有多种形式，包括数字型VLAN和字符型VLAN，字符型VLAN又可分为VLAN名称、VLAN组名。

服务器向设备下发授权VLAN信息后，设备首先对其进行解析，只要解析成功，即以对应的方法下发授权VLAN；如果解析不成功，则用户授权失败。

- 若认证服务器下发的授权VLAN信息为一个VLAN ID，则该VLAN是有效的授权VLAN。

- 若认证服务器下发的授权 VLAN 信息为一个 VLAN 名称，则仅当对应的 VLAN 存在时该 VLAN 才是有效的授权 VLAN。
- 若认证服务器下发的授权 VLAN 信息为一个 VLAN 组名，则设备首先会通过组名查找该组内配置的 VLAN 列表，然后将该组 VLAN 中 ID 最小的 VLAN 作为有效的授权 VLAN。关于 VLAN 组的相关配置，请参见“二层技术-以太网交换配置指导”中的“VLAN”。
- 若认证服务器下发的授权 VLAN 信息为一个包含若干 VLAN 编号以及若干 VLAN 名称的字符串，则设备首先将其解析为一组 VLAN ID，然后将该组 VLAN 中 ID 最小的 VLAN 作为有效的授权 VLAN。

解析出来有效的授权 VLAN 后，则需要进行下发。

由于授权信息是用来控制数据报文转发的，因此，授权信息必须在授权点下发。这也就意味着，在认证设备和授权设备分离场景下，用户在认证设备上获取授权信息后，认证设备需要将授权信息携带至授权设备下发。

基于上述考虑，下发的方式分为本地下发授权 VLAN 和远端下发授权 VLAN：

(1) 本地下发授权 VLAN

在认证设备和授权设备未分离场景下，在认证设备上获取用户授权 VLAN 信息后，直接在认证设备下发。

(2) 远端下发授权 VLAN

在认证设备和授权设备分离场景下，认证设备上获取用户授权 VLAN 信息后，需要将该信息发送至远端授权设备，授权信息在远端设备上解析后下发。

2. Fail VLAN

Fail VLAN 功能允许用户在认证失败的情况下访问某一特定 VLAN 中的资源，这个 VLAN 称之为 Fail VLAN。需要注意的是，这里的认证失败是指认证服务器因某种原因明确拒绝用户认证通过，比如用户名错误或密码错误，而不是认证超时或网络连接等原因造成的认证失败。需要注意的是，如果采用 RSNA 安全机制的 802.1X 用户认证失败，则用户会直接下线，不会加入认证失败 VLAN。

Fail VLAN 优先级高于入侵检测。因此，用户身份认证失败后，如果配置了 Fail VLAN 则加入 Fail VLAN；如果没有配置 Fail VLAN，再判断是否开始入侵检测功能，如果开启了，则出发入侵检测。如果既没有配置 Fail VLAN，也没有开启入侵检测功能，则不进行任何认证失败处理。

1.1.6 支持授权ACL下发

用户通过 802.1X 认证或 MAC 地址认证后，支持授权 ACL（Access Control List，访问控制列表）下发，授权 ACL（Access Control List，访问控制列表）下发提供了对上线用户访问网络资源的过滤与控制功能。当用户上线时，如果 RADIUS 服务器上或接入设备的本地用户视图中指定了要下发给该用户的授权 ACL，则设备会根据下发的授权 ACL 对用户数据流进行过滤，仅允许 ACL 规则中允许的数据流通过。由于服务器上或设备本地用户视图下指定的是授权 ACL 的编号，因此还需要在设备上创建该 ACL 并配置对应的 ACL 规则。管理员可以通过改变授权的 ACL 编号或设备上对应的 ACL 规则来改变用户的访问权限。

1.1.7 支持User Profile下发

用户通过 802.1X 认证或 MAC 地址认证后，支持授权 User Profile 下发，User Profile 下发提供了对上线用户访问网络资源的过滤与控制功能。当用户上线时，如果 RADIUS 服务器上或接入设备的

本地用户视图中指定了要下发给该用户的授权 User Profile，则设备会根据服务器下发的授权 User Profile 对用户所在端口的数据流进行过滤，仅允许 User Profile 策略中允许的数据流通过该端口。由于服务器上指定的是授权 User Profile 名称，因此还需要在设备上创建该 User Profile 并配置该对应的 User Profile 策略。管理员可以通过改变授权的 User Profile 名称或设备上对应的 User Profile 配置来改变用户的访问权限。

1.2 WLAN用户接入认证配置任务简介

表1-2 WLAN 用户接入认证配置任务简介

配置任务		说明	详细配置
配置全局认证参数	配置OUI	可选	1.4.1
	配置802.1X支持的域名分隔符	可选	1.4.2
	配置802.1X系统的认证方法	可选	1.4.3
	配置设备向接入用户发送认证请求报文最大次数	可选	1.4.4
	配置802.1X认证定时器	可选	1.4.5
	配置MAC地址认证用户名及密码格式	可选	1.4.6
	配置MAC地址认证用户使用的ISP域	可选	1.4.7
	配置MAC地址认证定时器	可选	1.4.8
配置WLAN用户接入认证参数	配置WLAN用户接入认证模式	必选	1.5.1
	配置802.1X认证的EAP协议模式	可选	1.5.2
	配置忽略MAC地址认证结果	可选	1.5.3
	配置URL重定向功能	可选	1.5.4
	配置认证失败VLAN	可选	1.5.5
	配置忽略授权信息	可选	1.5.6
	配置授权失败强制用户下线	可选	1.5.7
	配置入侵检测功能	可选	1.5.8
	配置 802.1X握手功能	可选	1.5.9
	配置802.1X安全握手功能	可选	1.5.10
	配置802.1X认证用户ISP域	可选	1.5.11
	配置802.1X最大用户数	可选	1.5.12
	配置802.1X重认证功能	可选	1.5.13
	配置MAC地址认证最大用户数	可选	1.5.14
	配置MAC地址认证用户ISP域	可选	1.5.15

1.3 配置准备

1. 802.1X认证配置准备

802.1X 需要 AAA 的配合才能实现对用户的身份认证。因此，需要首先完成以下配置任务：

- 配置 802.1X 用户所属的 ISP 域及其使用的 AAA 方案，即本地认证方案或 RADIUS 方案。
- 如果需要通过 RADIUS 服务器进行认证，则应该在 RADIUS 服务器上配置相应的用户名和密码。
- 如果需要本地认证，则应该在设备上手动添加认证的用户名和密码。配置本地认证时，用户使用的服务类型必须设置为 **lan-access**。

2. MAC地址认证配置准备

缺省情况下，对接入的用户进行 MAC 地址认证时，使用系统缺省的 ISP 域（由命令 **domain default enable** 指定）。若需要使用非缺省的 ISP 域进行 MAC 地址认证，则需指定 MAC 地址认证用户使用的 ISP 域，并配置该 ISP 域。ISP 域的具体配置请参见“安全配置指导”中的“AAA”。

- 若采用本地认证方式，还需创建本地用户并设置其密码，且本地用户的服务类型应设置为 **lan-access**。
- 若采用远程 RADIUS 认证方式，需要确保设备与 RADIUS 服务器之间的路由可达，并添加 MAC 地址认证的用户帐号。

1.4 配置全局认证参数

1.4.1 配置OUI

目前设备支持配置最多 16 个 OUI。

表1-3 配置 OUI

操作	命令	说明
进入系统视图	**system-view**	-
配置允许通过认证的用户OUI值	**port-security oui index** *index-value* **mac-address** *oui-value*	仅在用户接入认证模式为**oui-then-dot1x**的情况下必选 缺省情况下，不存在允许通过认证的用户OUI值 允许通过认证的用户OUI值可以配置多个 本命令的详细介绍，请参见“安全命令参考”中的“端口安全”

1.4.2 配置 802.1X支持的域名分隔符

有关 802.1X 支持的域名分隔符的详细介绍请参见“安全配置指导”中的“802.1X”。

表1-4 配置 802.1X 支持的域名分隔符

配置步骤	命令	说明
进入系统视图	**system-view**	-
指定802.1X支持的域名分隔符	**dot1x domain-delimiter** *string*	缺省情况下，仅支持域名分隔符@ 本命令的详细介绍，请参见“安全命令参考”中的“802.1X”

1.4.3 配置 802.1X系统的认证方法

有关 802.1X 系统的认证方法的详细介绍请参见“安全配置指导”中的“802.1X”。

表1-5 配置 802.1X 系统的认证方法

配置步骤	命令	说明
进入系统视图	**system-view**	-
配置802.1X系统的认证方法	**dot1x authentication-method { chap | eap | pap }**	缺省情况下，设备启用EAP终结方式，并采用CHAP认证方法 本命令的详细介绍，请参见“安全命令参考”中的“802.1X”

说明

如果采用 EAP 中继认证方式，则设备会把客户端输入的内容直接封装后发给服务器，这种情况下 **user-name-format** 命令的设置无效，**user-name-format** 的介绍请参见“安全命令参考”中的“AAA”。

1.4.4 配置设备向接入用户发送认证请求报文最大次数

有关设备向接入用户发送认证请求报文最大次数的详细介绍请参见“安全配置指导”中的“802.1X”。

表1-6 配置设备向接入用户发送认证请求报文的最大次数

配置步骤	命令	说明
进入系统视图	**system-view**	-
配置设备向接入用户发送认证请求报文的最大次数	**dot1x retry** *max-retry-value*	缺省情况下，设备最多可向接入用户发送2次认证请求报文 本命令的详细介绍，请参见“安全命令参考”中的“802.1X”

1.4.5 配置 802.1X定时器

802.1X 认证过程中会启动多个定时器以控制客户端、设备以及 RADIUS 服务器之间进行合理、有序的交互。可配置的 802.1X 认证定时器包括以下四种：

- 客户端认证超时定时器：当设备向客户端发送了 EAP-Request/MD5 Challenge 请求报文后，设备启动此定时器，若在该定时器设置的时长内，设备没有收到客户端的响应，设备将重发该报文。若在 **dot1x retry** 命令配置的次数内，没有收到客户端响应，则客户端认证失败。
- 认证服务器超时定时器：当设备向认证服务器发送了 RADIUS Access-Request 请求报文后，设备启动该定时器，若在该定时器设置的时长内，设备没有收到认证服务器的响应，设备将重发认证请求报文。
- 握手定时器：用户认证成功之后，如果开启了握手功能，该定时器将启动。设备会以该定时器配置的时间为周期向用户发送握手报文，若在该定时器设置的时间内，设备没有收到客户端的回应报文，设备将重发该握手报文，若在 **dot1x retry** 命令配置的次数内，没有收到客户端回应，则强制该客户端下线。
- 周期性重认证定时器：如果设备开启了周期认证功能，设备将以该定时器配置的时间为周期发起重认证。配置该定时器后，对于新上线的 802.1X 用户，会按新配置的重认证周期进行重认证，对于已经在线的用户，新配置不会生效。

一般情况下，无需改变定时器的值，除非在一些特殊或恶劣的网络环境下，才需要通过命令来调节。例如，用户网络状况比较差的情况下，可以适当地将客户端认证超时定时器值调大一些；还可以通过调节认证服务器超时定时器的值来适应不同认证服务器的性能差异。

表1-7 配置 802.1X 认证定时器

配置步骤	命令	说明
进入系统视图	**system-view**	-
配置客户端认证超时定时器	**dot1x timer supp-timeout** *supp-timeout-value*	缺省情况下，客户端认证超时定时器的值为30秒 本命令的详细介绍，请参见“安全命令参考”中的“802.1X”
配置认证服务器超时定时器	**dot1x timer server-timeout** *server-timeout-value*	缺省情况下，认证服务器超时定时器的值为100秒 本命令的详细介绍，请参见“安全命令参考”中的“802.1X”
配置握手定时器	**dot1x timer handshake-period** *handshake-period-value*	缺省情况下，握手定时器的值为15秒 本命令的详细介绍，请参见“安全命令参考”中的“802.1X”
配置周期性重认证定时器	**dot1x timer reauth-period** *reauth-period-value*	缺省情况下，周期性重认证定时器的值为3600秒 本命令的详细介绍，请参见“安全命令参考”中的“802.1X”

1.4.6 配置MAC地址认证用户名及密码格式

表1-8 配置 MAC 地址认证用户名格式

操作		命令	说明
进入系统视图		**system-view**	-
配置MAC地址认证用户的用户名格式	MAC地址格式	**mac-authentication user-name-format mac-address** [{ **with-hyphen** | **without-hyphen** } [**lowercase** | **uppercase**]]	二者选其一 缺省情况下，使用用户的MAC地址作为用户名与密码，其中字母为小写，且不带连字符“-” 本命令的详细介绍，请参见“安全命令参考”中的“MAC地址认证”
	固定用户名格式	**mac-authentication user-name-format fixed** [**account** *name*] [**password** { **cipher** | **simple** } *password*]	

1.4.7 配置MAC地址认证用户使用的ISP域

为了便于接入设备的管理员更为灵活地部署用户的接入策略，设备支持指定 MAC 地址认证用户使用的 ISP 域。关于 ISP 域的详细介绍，请参见“安全配置指导”中的“AAA”。

表1-9 指定 MAC 地址认证用户使用的 ISP 域

配置步骤	命令	说明
进入系统视图	**system-view**	-
指定MAC地址认证用户使用的ISP域	**mac-authentication domain** *domain-name*	缺省情况下，未指定MAC地址认证用户使用的ISP域 从无线服务模板上接入的MAC地址认证用户将按照如下先后顺序进行选择ISP域：无线服务模板下指定的ISP域-->全局MAC地址ISP域-->系统缺省的ISP域 本命令的详细介绍，请参见“安全命令参考”中的“MAC地址认证”

1.4.8 配置MAC地址认证定时器

可配置的 MAC 地址认证定时器目前只有一种：

服务器超时定时器（**server-timeout**）：用来设置设备同 RADIUS 服务器的连接超时时间。在用户的认证过程中，如果到服务器超时定时器超时时设备一直没有收到 RADIUS 服务器的应答，则设备将禁止此用户访问网络。

表1-10 配置 MAC 地址认证定时器

操作	命令	说明
进入系统视图	**system-view**	-
配置MAC地址认证定时器	**mac-authentication timer server-timeout** *server-timeout-value*	缺省情况下，服务器超时定时器取值为100秒 本命令的详细介绍，请参见“安全命令参

操作	命令	说明
		考”中的“MAC地址认证”

1.5 配置WLAN用户认证接入认证参数

1.5.1 配置WLAN用户接入认证模式

表1-11 配置 WLAN 用户接入认证模式

操作	命令	说明
进入系统视图	**system-view**	-
进入无线服务模板视图	**wlan service-template** *service-template-name*	-
配置WLAN用户接入认证模式	**client-security authentication-mode** { **dot1x** | **dot1x-then-mac** | **mac** | **mac-then-dot1x** | **oui-then-dot1x** }	缺省情况下，不对用户进行认证即Bypass认证，直接接入

1.5.2 配置 802.1X认证的EAP协议模式

配置 802.1X 认证的 EAP 协议模式，可以控制客户端和设备使用的 EAP 协议规范和报文格式。802.1X 认证的 EAP 协议模式：

- **extended**：表示 EAP 协议模式为扩展的 EAP 协议，即要求客户端和设备按照私有 EAP 协议的规范和报文格式进行交互。
- **standard**：表示 EAP 协议模式为标准的 EAP 协议，即要求客户端和设备按照标准 EAP 协议的规范和报文格式进行交互。

仅当使用 iMC 作为 RADIUS 服务器时，需要配置 802.1X 认证的 EAP 协议模式：如果采用 H3C iNode 作为 802.1X 客户端，则配置 EAP 协议模式为 **extended**；如果采用其它类型的 802.1X 客户端，则配置 EAP 协议模式为 **standard**。

表1-12 配置 802.1X 认证的 EAP 协议模式

操作	命令	说明
进入系统视图	**system-view**	-
进入无线服务模板视图	**wlan service-template** *service-template-name*	-
配置802.1X认证的EAP协议模式	**dot1x eap** { **extended** | **standard** }	缺省情况下，EAP协议模式为**standard**

1.5.3 配置忽略MAC地址认证结果

说明

本功能仅适用于客户端采用 RADIUS 服务器认证方式进行的 MAC 地址认证。

如果同时配置了 MAC 地址认证和 Portal 认证，则无线用户须依次通过 MAC 地址认证和 Portal 认证才能访问网络资源，且用户每次都需要输入 Portal 认证的用户名和密码才能完成认证。配置忽略 MAC 地址认证结果，可以简化上述认证操作。设备开启忽略 MAC 地址认证结果功能后，具体认证过程如下：

- 若 RADIUS 服务器上已经记录了用户和其 MAC 地址的对应信息，则用户通过 MAC 地址认证，且不再需要进行 Portal 认证即可访问网络资源。
- 若 RADIUS 服务器上未记录用户和其 MAC 地址的对应信息，则 MAC 地址认证失败。此时，设备忽略这一认证结果，直接进行 Portal 认证。Portal 认证通过后即可访问网络资源，同时 RADIUS 服务器将记录该用户和其 MAC 地址的对应信息。此后，该用户仅需要完成 MAC 地址认证即可访问网络资源，而不再需要进行 Portal 认证。

表1-13 配置忽略 MAC 地址认证结果

操作	命令	说明
进入系统视图	**system-view**	-
进入无线服务模板视图	**wlan service-template** *service-template-name*	-
配置忽略MAC地址认证结果	**client-security ignore-authentication**	缺省情况下，应用MAC地址认证结果

1.5.4 配置URL重定向功能

说明

本功能仅适用于客户端采用 RADIUS 服务器认证方式进行的 MAC 地址认证。

在用户进行 MAC 地址认证上线过程中，如果 RADIUS 服务器上没有记录用户及其 MAC 地址的对应信息，但仍需要用户进行认证时，可以通过在设备上开启 URL 重定向功能。开启后，用户可以根据 RADIUS 服务器下发的重定向 URL，跳转到指定的 Web 认证界面进行用户认证。用户认证通过后，RADIUS 服务器将记录用户的 MAC 地址信息，并通过 DM 报文强制用户下线，此后该用户即可正常完成 MAC 地址认证。有关 DM 报文的详细介绍请参见“安全配置指导”中的“AAA”。

设备开启 URL 重定向功能后，MAC 地址认证过程如下：

(1) RADIUS 服务器下发授权 ACL 和重定向 URL。

(2) 用户试图通过 HTTP 访问外网时，该 HTTP 请求会匹配授权 ACL 的 deny 规则，然后该请求会被重定向到重定向 URL 所指向的认证页面。

(3) 在认证页面，用户输入运营商提供的用户名和密码，完成 Web 页面认证并记录该用户及其 MAC 地址的对应信息。

(4) 认证完成后，RADIUS 服务器通过发送 DM 请求报文强制用户下线。

(5) 用户下线后，再次进行 MAC 地址认证，由于 RADIUS 服务器上已记录该用户及其 MAC 地址的对应信息，用户可以完成 MAC 地址认证。

在 RADIUS 服务器或接入设备上配置授权 ACL 和重定向 URL 时有如下注意事项：

- 授权 ACL 需要允许客户端与认证页面交互的报文通过。有关授权 ACL 的详细介绍请参见“安全配置指导”中的“MAC 地址认证”。
- 若无线客户端通过 DHCP 动态获取 IP 地址，则授权 ACL 需要允许无线客户端与 DHCP 服务器交互的报文通过；若采用手工方式配置 IP 地址，则无此限制。
- 其他报文缺省不允许通过。
- 重定向 URL 即为用户进行用户认证时 Web 页面的地址。

表1-14 配置 URL 重定向功能

操作	命令	说明
进入系统视图	**system-view**	-
进入无线服务模板视图	**wlan service-template** *service-template-name*	-
配置URL重定向功能	**client url-redirect enable**	缺省情况下，客户端URL重定向功能处于关闭状态

1.5.5 配置认证失败VLAN

如果配置了认证失败 VLAN，认证失败的用户将被加入该 VLAN，同时设备会启动一个 30 秒的定时器，以定期对用户进行重新认证。如果重认证通过，设备将根据 AAA 服务器是否下发 VLAN 来重新指定该用户所在 VLAN，即如果 AAA 服务器下发了 VLAN，则该用户将被加入该下发的 VLAN，否则该用户将被加入其原来所属的 VLAN；如果重认证未通过，则该用户仍然留在认证失败 VLAN 中。

表1-15 配置认证失败 VLAN

操作	命令	说明
进入系统视图	**system-view**	-
进入无线服务模板视图	**wlan service-template** *service-template-name*	-
配置认证失败VLAN	**client-security authentication fail-vlan** *vlan-id*	缺省情况下，没有配置认证失败VLAN

1.5.6 配置忽略授权信息

授权信息包括 VLAN、ACL 和 User Profile，分为 RADIUS 服务器下发的授权信息和设备本地下发的授权信息。若用户不想使用授权信息，则可以配置忽略授权信息。

表1-16 配置忽略授权信息

操作	命令	说明
进入系统视图	**system-view**	-
进入无线服务模板视图	**wlan service-template** *service-template-name*	-
配置忽略RADIUS服务器或设备本地下发的授权信息	**client-security ignore-authorization**	缺省情况下，应用RADIUS服务器或设备本地下发的授权信息

1.5.7 配置授权失败强制用户下线

如果开启了授权失败后的用户下线功能，当下发的授权 ACL、User Profile 不存在、已授权 ACL、User Profile 被删除，或者 ACL、User Profile 下发失败时，将强制用户下线；

如果没有开启授权失败后的用户下线功能，当下发的授权 ACL、User Profile 不存在、已授权 ACL、User Profile 被删除，或者 ACL、User Profile 下发失败时，用户保持在线，授权 ACL、User Profile 不生效，设备打印 Log 信息。

需要注意的是，对于授权 VLAN 失败的情况下，设备会直接让用户下线，与此功能无关。

表1-17 配置授权失败强制用户下线

操作	命令	说明
进入系统视图	**system-view**	-
进入无线服务模板视图	**wlan service-template** *service-template-name*	-
配置授权失败强制用户下线	**client-security authorization-fail offline**	缺省情况下，设置授权信息失败后，用户保持在线

1.5.8 配置入侵检测功能

当检测到一个非法用户试图访问网络时，如果开启了入侵检测功能，设备将对其所在的BSS采取相应的安全模式。有关安全模式的详细介绍，请参见“1.1.3 入侵检测”。

表1-18 配置入侵检测功能

操作	命令	说明
进入系统视图	**system-view**	-
进入无线服务模板视图	**wlan service-template** *service-template-name*	-
配置入侵检测功能	**client-security intrusion-protection enable**	缺省情况下，入侵保护功能处于关闭状态
（可选）配置入侵检测模式	**client-security intrusion-protection action { service-stop | temporary-block | temporary-service-stop }**	缺省情况下，入侵检测模式为**temporary-block**模式
（可选）配置临时阻塞非法入侵用户时长	**client-security intrusion-protection timer temporary-block** *time*	缺省情况下，临时阻塞非法入侵用户时间为180秒

操作	命令	说明
（可选）配置临时关闭BSS服务时长	**client-security intrusion-protection timer temporary-service-stop** *time*	缺省情况下，临时关闭BSS服务时长为20秒

1.5.9 配置 802.1X握手功能

使能 802.1X 握手功能之后，设备将定期向通过 802.1X 认证的在线用户发送握手报文，即单播 EAP-Request/Identity 报文，来检测用户的在线状态。握手报文发送的时间间隔由 802.1X 握手定时器控制（时间间隔通过命令 **dot1x timer handshake-period** 设置）。如果连续发送握手报文的次数达到 802.1X 报文最大重发次数，而还没有收到用户响应，则强制该用户下线。

表1-19 配置 802.1X 握手功能

操作	命令	说明
进入系统视图	**system-view**	-
进入无线服务模板视图	**wlan service-template** *service-template-name*	-
配置802.1X在线用户握手功能	**dot1x handshake enable**	缺省情况下，无线服务模板下的802.1X在线用户握手功能处于关闭状态

1.5.10 配置 802.1X安全握手功能

802.1X 安全握手是指在握手报文中加入验证信息，以防止非法用户仿冒正常用户的在线的 802.1X 的客户端与设备进行握手报文的交互。使能 802.1X 安全握手功能后，支持安全握手的客户端需要在每次向设备发送的握手应答报文中携带验证信息，设备将其与认证服务器下发的验证信息进行对比，如果不一致，则强制用户下线。

验证信息由认证服务器下发，当用户上线认证成功时，服务器在认证回复报文中携带验证密钥和验证信息。设备保存验证信息，而将验证密钥发送给客户端。之后，当用户需要响应设备的握手报文时，首先使用验证密钥计算出一个验证信息，然后将该验证信息携带在握手回应报文 EAPOL EAP-Response Identity 中发给设备。

服务器会周期性地更新验证密钥与验证信息，并通过计费响应报文下发给设备。设备同样会将验证密钥发送给客户端，而保存验证信息用于校验客户端响应报文的合法性。

表1-20 配置 802.1X 安全握手功能

操作	命令	说明
进入系统视图	**system-view**	-
进入无线服务模板视图	**wlan service-template** *service-template-name*	-
配置802.1X在线用户握手功能	**dot1x handshake enable**	缺省情况下，无线服务模板下的802.1X在线用户握手功能处于关闭状态
配置802.1X在线用户安全握手功能	**dot1x handshake secure enable**	缺省情况下，802.1X的在线用户的安全握手功能处于关闭状态

说明

- 802.1X 安全握手功能只有在使能了 802.1X 握手功能的前提下才生效。
- **dot1x handshake secure enable** 命令只对进行 802.1X 认证且成功上线的用户有效。

1.5.11 配置 802.1X认证用户ISP域

从无线服务模板上接入的 802.1X 用户将按照如下先后顺序进行选择 ISP 域：无线服务模板下指定的 ISP 域-->用户名中指定的 ISP 域-->系统缺省的 ISP 域。

表1-21 配置 802.1x 用户 ISP 域

操作	命令	说明
进入系统视图	**system-view**	-
进入无线服务模板视图	**wlan service-template** *service-template-name*	-
配置802.1X用户ISP域	**dot1x domain** *domain-name*	缺省情况下，未指定无线服务模板下的802.1X用户的ISP域

1.5.12 配置 802.1X最大用户数

当接入此无线服务模板的 802.1X 用户数超过最大值后，新接入的用户将被拒绝。

表1-22 配置 802.1x 最大用户数

操作	命令	说明
进入系统视图	**system-view**	-
进入无线服务模板视图	**wlan service-template** *service-template-name*	-
配置802.1X最大用户数	**dot1x max-user** *count*	缺省情况下，当前无线服务模板上允许同时接入的802.1X用户数为4096个

1.5.13 配置 802.1X重认证功能

在无线服务模板下启动了 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设定的时间间隔（由命令 **dot1x timer reauth-period** 设置）定期向在线 802.1X 用户发起重认证，以检测用户连接状态的变化、确保用户的正常在线，并及时更新服务器下发的授权属性（例如 ACL、VLAN、User Profile）。

认证服务器可以通过下发 RADIUS 属性（session-timeout、termination-action）来指定用户会话超时时长以及会话中止的动作类型。认证服务器上如何下发以上 RADIUS 属性的具体配置以及是否可以下发重认证周期的情况与服务器类型有关，请参考具体的认证服务器实现。

802.1X 用户认证通过后，用户的重认证功能具体实现如下：

- 当认证服务器下发了用户会话超时时长，且指定的会话中止动作为要求用户进行重认证，则无论设备上是否开启周期性重认证功能，都会在用户会话超时时长到达后对该用户发起重认证。
- 当认证服务器下发了用户会话超时时长，且指定的会话中止动作为要求用户下线时：
  - 若设备上开启了周期性重认证功能，且设备上配置的重认证定时器值小于用户会话超时时长，则用户会以重认证定时器的值为周期发起重认证；若设备上配置的重认证定时器值大于等于用户会话超时时长，则在用户会话超时时长到达后下线。
  - 若设备上未开启周期性重认证功能，则用户在会话超时时长到达后下线。
- 当认证服务器未下发用户会话超时时长时，是否对用户进行重认证，由设备上配置的重认证功能决定。

表1-23 配置 802.1x 重认证功能

操作	命令	说明
进入系统视图	**system-view**	-
进入无线服务模板视图	**wlan service-template** *service-template-name*	-
配置802.1X重认证功能	**dot1x re-authenticate enable**	缺省情况下，无线服务模板上的802.1X周期性重认证功能处于关闭状态

1.5.14 配置MAC地址认证最大用户数

当接入此无线服务模板的 MAC 地址认证用户数超过最大值后，新接入的用户将被拒绝。

表1-24 配置 MAC 地址认证最大用户数

操作	命令	说明
进入系统视图	**system-view**	-
进入无线服务模板视图	**wlan service-template** *service-template-name*	-
配置MAC地址认证最大用户数	**mac-authentication max-user** *count*	缺省情况下，当前无线服务模板上允许接入的MAC地址认证最大用户数为4096个

1.5.15 配置MAC地址认证用户ISP域

从无线服务模板上接入的 MAC 地址认证用户将按照如下先后顺序进行选择 ISP 域：无线服务模板下指定的 ISP 域-->全局 MAC 地址 ISP 域-->系统缺省的 ISP 域。

表1-25 配置 MAC 地址认证用户 ISP 域

操作	命令	说明
进入系统视图	**system-view**	-
进入无线服务模板视图	**wlan service-template** *service-template-name*	-

操作	命令	说明
配置MAC地址认证用户的ISP域	**mac-autentication domain** *domain-name*	缺省情况下，未指定无线服务模板下的MAC地址认证用户的ISP域

1.6 WLAN用户接入认证显示和维护

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用户接入认证的运行情况，通过查看显示信息验证配置的效果。

在用户视图下，执行 **reset** 命令可以清除相关统计信息。

display dot1x connection、**display dot1x** 和 **reset dot1x statistics** 命令的详细介绍，请参见“安全命令参考”中的“802.1X”。

display mac-authentication connection 、 **display mac-authentication** 和 **reset mac-authentication statistics** 命令的详细介绍，请参见“安全命令参考”中的“MAC 地址认证”。

表1-26 WLAN 用户接入认证显示和维护

操作	命令
显示802.1X在线用户的连接信息	**display dot1x connection** [**interface** *interface-type interface-number* | **user-mac** *mac-addr* | **user-name** *name-string*]
显示802.1X的会话连接信息、相关统计信息或配置信息	**display dot1x** [**sessions** | **statistics**] [**interface** *interface-type interface-number*]
显示MAC地址认证连接信息	**display mac-authentication connection** [**interface** *interface-type interface-number* | **user-mac** *mac-addr* | **user-name** *name-string*]
显示MAC地址认证的相关信息	**display mac-authentication** [**interface** *interface-type interface-number*]
显示阻塞MAC地址信息	**display wlan client-security block-mac**
清除802.1X的统计信息	**reset dot1x statistics** [**interface** *interface-type interface-number*]
清除MAC地址认证的统计信息	**reset mac-authentication statistics** [**interface** *interface-type interface-number*]

1.7 WLAN用户接入认证典型配置举例

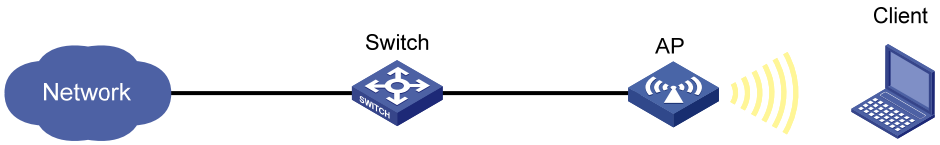
1.7.1 802.1X认证（CHAP非加密本地认证）典型配置举例

1. 组网需求

如 图 1-5 所示，客户端使用本地 802.1X认证CHAP方式接入无线网络，

2. 组网图

图1-5 802.1X 认证（CHAP 非加密本地认证）典型配置组网图



3. 配置步骤

说明

下述配置步骤中包含了若干 AAA/本地用户的配置命令，关于这些命令的详细介绍请参见“安全命令参考”中的“AAA”。

(1) 配置 802.1X 认证方式及本地用户

配置 802.1X 认证方式为 CHAP。

```
<AP> system-view
[AP] dot1x authentication-method chap
```

配置本地用户，用户名为 chap1，所属的组为网络接入用户组，密码为明文 123456，服务类型为 lan-access。

```
[AP] local-user chap1 class network
[AP-luser-network-chap1] password simple 123456
[AP-luser-network-chap1] service-type lan-access
[AP-luser-network-chap1] quit
```

(2) 配置 ISP 域的 AAA 方法

配置名称为 local 的 ISP 域，并将认证、授权和计费的方式配置为本地。

```
[AP] domain local
[AP-isp-local] authentication lan-access local
[AP-isp-local] authorization lan-access local
[AP-isp-local] accounting lan-access local
[AP-isp-local] quit
```

(3) 配置无线服务模板

配置无线服务模板，名称为 wlas_local_chap，用户认证方式为 802.1X，ISP 域为 local，SSID 为 wlas_local_chap。

```
[AP] wlan service-template wlas_local_chap
[AP-wlan-st-wlas_local_chap] client-security authentication-mode dot1x
[AP-wlan-st-wlas_local_chap] dot1x domain local
[AP-wlan-st-wlas_local_chap] ssid wlas_local_chap
```

使能无线服务模板。

```
[AP-wlan-st-wlas_local_chap] service-template enable
[AP-wlan-st-wlas_local_chap] quit
```

(4) 将无线服务模板绑定到 WLAN-Radio 1/0/1 接口上

```
[AP] interface wlan-radio 1/0/1
```

```
[AP-WLAN-Radio1/0/1] undo shutdown
[AP-WLAN-Radio1/0/1] service template wlas_local_chap
[AP-WLAN-Radio1/0/1] quit
```

4. 验证结果

使用命令 **display wlan service-template** 和 **display dot1x** 命令可以查看 AP 上的 802.1X 配置情况。当 802.1X 用户输入正确的用户名和密码成功上线后，可使用命令 **display dot1x connection** 查看到上线用户的连接情况。

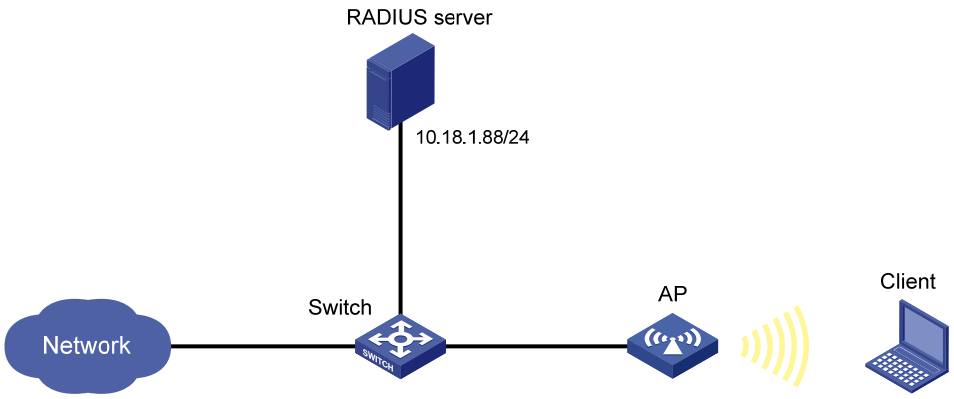
1.7.2 802.1X认证（EAP-PEAP加密）典型配置举例

1. 组网需求

- AP 和 RADIUS 服务器通过交换机建立连接，RADIUS 服务器的 IP 地址为 10.18.1.88。
- 要求使用 EAP-PEAP 方式进行远程 802.1X 用户身份认证。

2. 组网图

图1-6 802.1X 认证（EAP-PEAP 加密）典型配置组网图



3. 配置步骤

说明

- 下述配置步骤中包含了若干 AAA/RADIUS 协议的配置命令，关于这些命令的详细介绍请参见“安全配置指导”中的“AAA”。
- 完成 RADIUS 服务器的配置，安装证书并添加用户账户，保证用户的认证/授权/计费功能正常运行。
- 完成客户端 802.1X 的配置，安装证书。

(1) 配置 802.1X 认证方式及 RADIUS 方案

配置 802.1X 认证方式为 EAP。

```
<AP> system-view
[AP] dot1x authentication-method eap
```

配置 RADIUS 方案，名称为 imcc，主认证服务器的 IP 地址为 10.18.1.88，端口号为 1812，配置主计费服务器的 IP 地址为 10.18.1.88，端口号为 1813，认证密钥为明文 12345678，计费密钥为明文 12345678，用户名格式为 without-domain。

```
[AP] radius scheme imcc
[AP-radius-imcc] primary authentication 10.18.1.88 1812
[AP-radius-imcc] primary accounting 10.18.1.88 1813
[AP-radius-imcc] key authentication simple 12345678
[AP-radius-imcc] key accounting simple 12345678
[AP-radius-imcc] user-name-format without-domain
[AP-radius-imcc] quit
```

(2) 配置 ISP 域的 AAA 方法

配置名称为 imc 的 ISP 域，并将认证、授权和计费的方式配置为使用 RADIUS 方案 imcc。

```
[AP] domain imc
[AP-isp-imc] authentication lan-access radius-scheme imcc
[AP-isp-imc] authorization lan-access radius-scheme imcc
[AP-isp-imc] accounting lan-access radius-scheme imcc
[AP-isp-imc] quit
```

(3) 配置无线服务模板

配置无线服务模板名称为 wlas_imc_peap，用户认证方式为 802.1X，ISP 域为 imc，SSID 为 wlas_imc_peap，AKM 模式为 802.1X，加密套件为 CCMP，安全 IE 为 RSN。

```
[AP] wlan service-template wlas_imc_peap
[AP-wlan-st-wlas_imc_peap] client-security authentication-mode dot1x
[AP-wlan-st-wlas_imc_peap] dot1x domain imc
[AP-wlan-st-wlas_imc_peap] ssid wlas_imc_peap
[AP-wlan-st-wlas_imc_peap] akm mode dot1x
[AP-wlan-st-wlas_imc_peap] cipher-suite ccmp
[AP-wlan-st-wlas_imc_peap] security-ie rsn
```

使能无线服务模板。

```
[AP-wlan-st-wlas_imc_tls] service-template enable
[AP-wlan-st-wlas_imc_tls] quit
```

(4) 将无线服务模板绑定到 WLAN-Radio 1/0/1 接口上

```
[AP] interface wlan-radio 1/0/1
[AP-WLAN-Radio1/0/1] undo shutdown
[AP-WLAN-Radio1/0/1] service template wlas_local_chap
[AP-WLAN-Radio1/0/1] quit
```

(5) 配置 RADIUS server（iMC V7）

说明

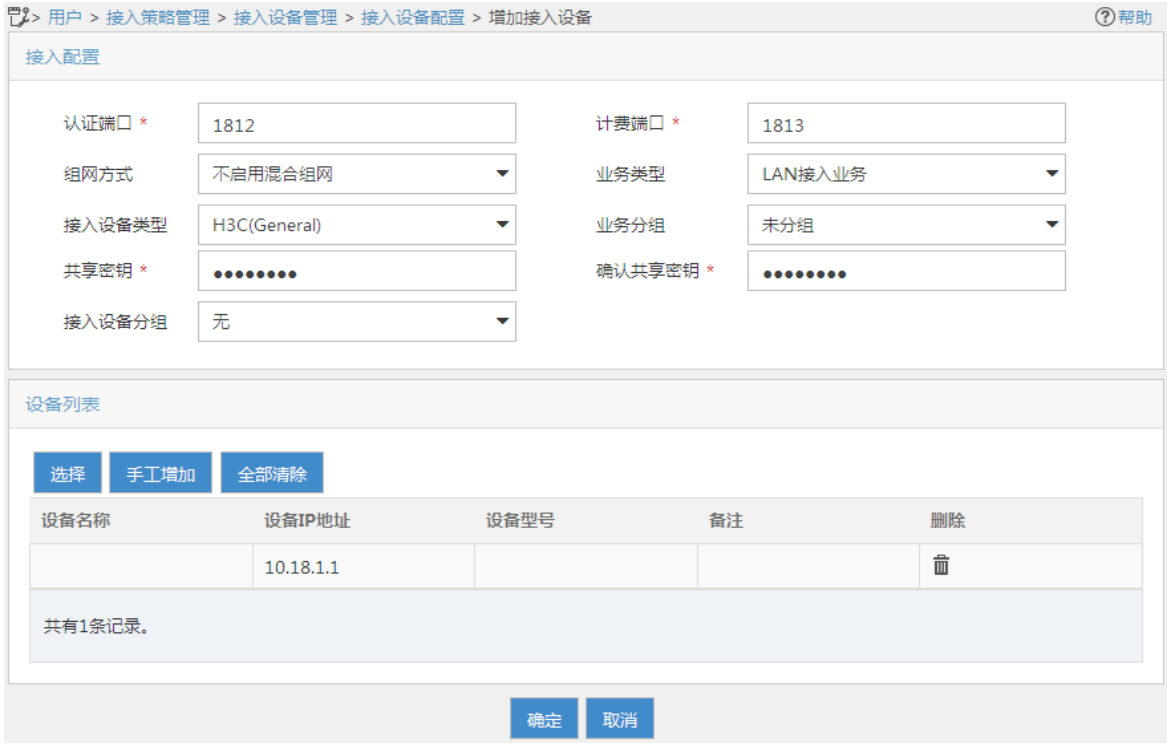
- 下面以 iMC 为例（使用 iMC 版本为：iMC PLAT 7.1、iMC UAM 7.1），说明 RADIUS server 的基本配置。
- 在服务器上已经完成证书的安装。

增加接入设备。

登录进入 iMC 管理平台，选择“用户”页签，单击导航树中的[接入策略管理/接入设备管理/接入设备配置]菜单项，进入接入设备配置页面，在该页面中单击“增加”按钮，进入增加接入设备页面。

- 设置认证、计费共享密钥为 12345678，其它保持缺省配置；
- 选择或手工增加接入设备，添加 IP 地址为 10.18.1.1 的接入设备。

图1-7 增加接入设备页面

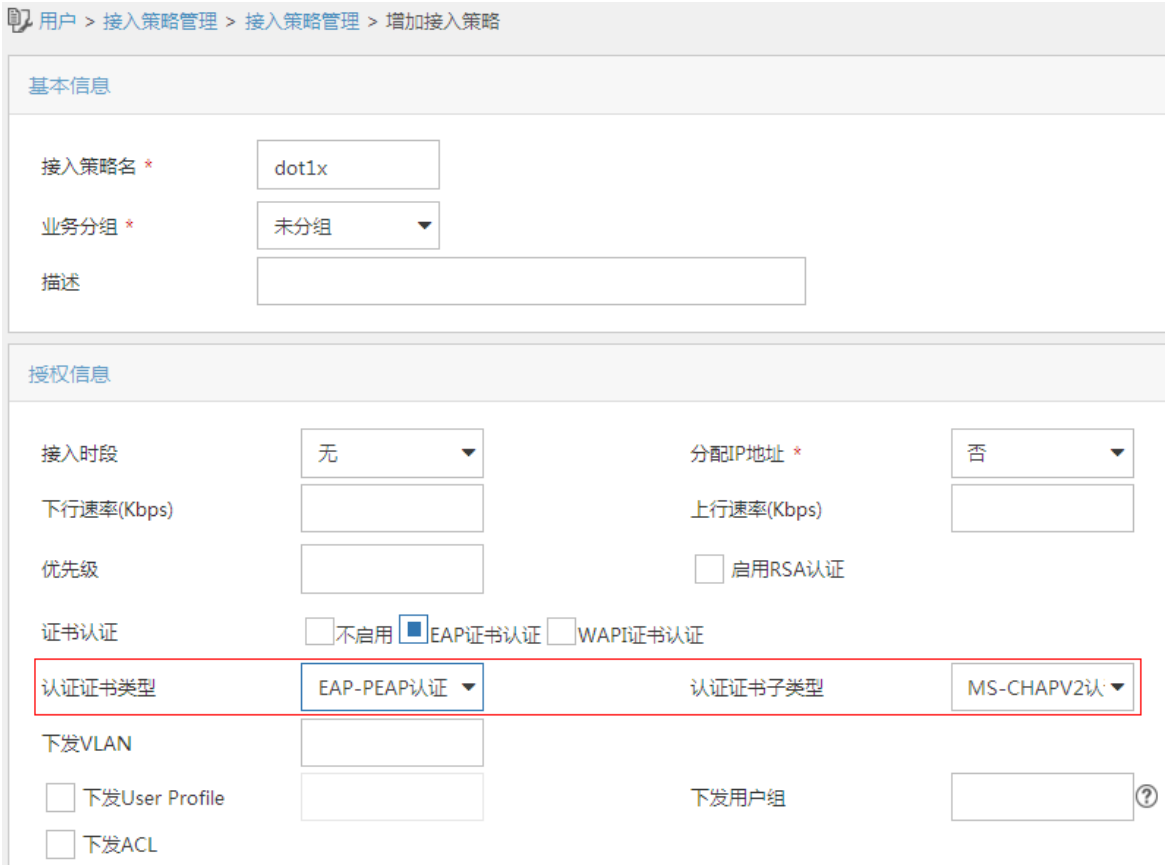


增加服务策略。

选择“用户”页签，单击导航树中的[接入策略管理/接入策略管理]菜单项，进入接入策略管理页面，在该页面中单击“增加”按钮，进入增加接入策略页面。

- 设置接入策略名为 dot1x；
- 选择认证证书类型为 EAP-PEAP 认证，认证证书子类型为 MS-CHAPV2 认证。认证证书子类型需要与客户端的身份验证方法一致。

图1-8 增加服务策略页面

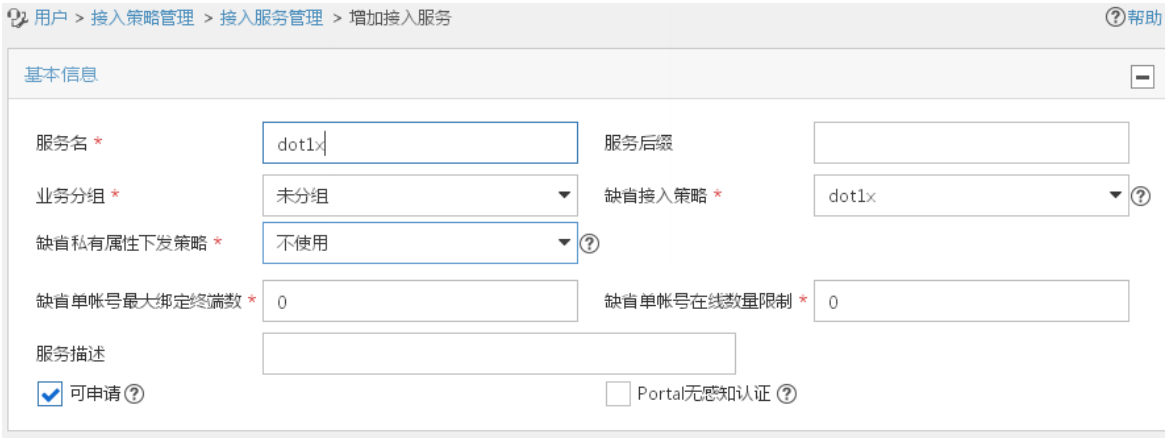


增加接入服务。

选择“用户”页签，单击导航栏中的[接入策略管理/接入服务管理]菜单项，进入接入服务管理页面，在该页面中单击<增加>按钮，进入增加接入服务页面。

- 设置服务名为 dot1x；
- 设置缺省接入策略为已经创建的 dot1x 策略。

图1-9 增加接入服务页面

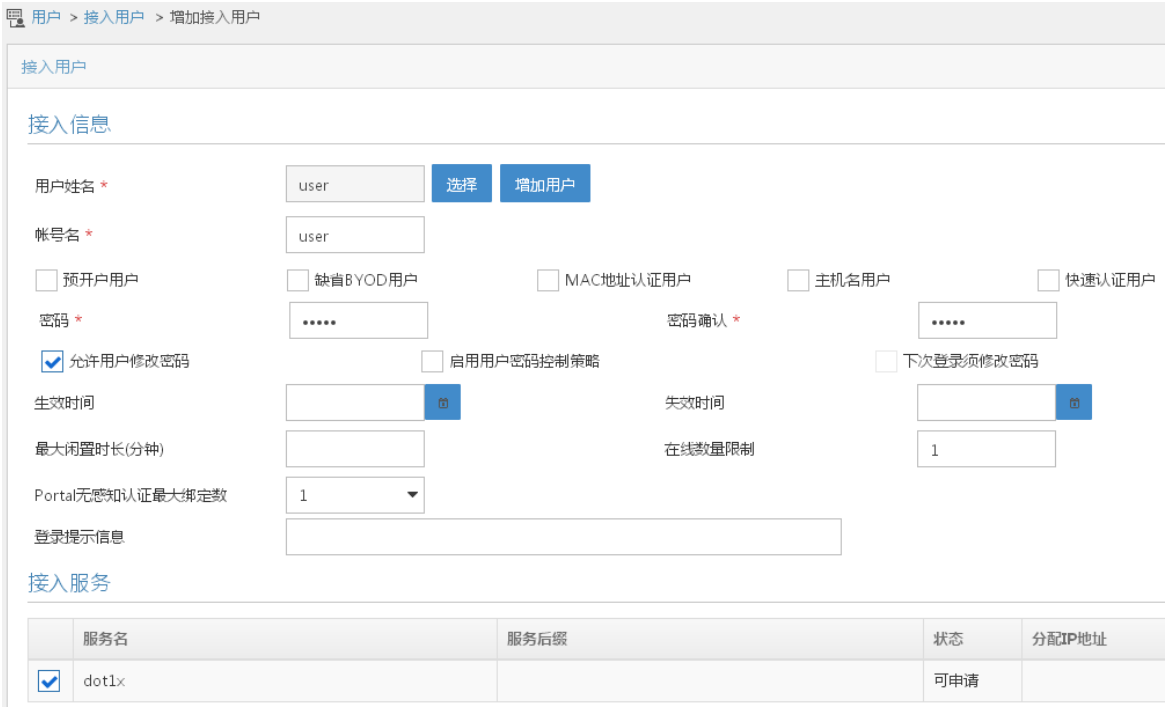


增加接入用户。

选择“用户”页签，单击导航树中的[接入用户管理/接入用户]菜单项，进入接入用户页面，在该页面中单击<增加>按钮，进入增加接入用户页面。

- 添加用户 user；
- 添加帐号名为 user，密码为 dot1x；
- 选中刚才配置的服务 dot1x。

图1-10 增加接入用户页面



(6) 配置无线网卡

选择无线网卡，在验证对话框中，选择 EAP 类型为 PEAP，点击“属性”，去掉验证服务器证书选项（此处不验证服务器证书），点击“配置”，去掉自动使用 Windows 登录名和密码选项。然后“确定”。整个过程如下图所示。

说明

在客户端上已经完成证书安装。

图1-11 无线网卡配置过程

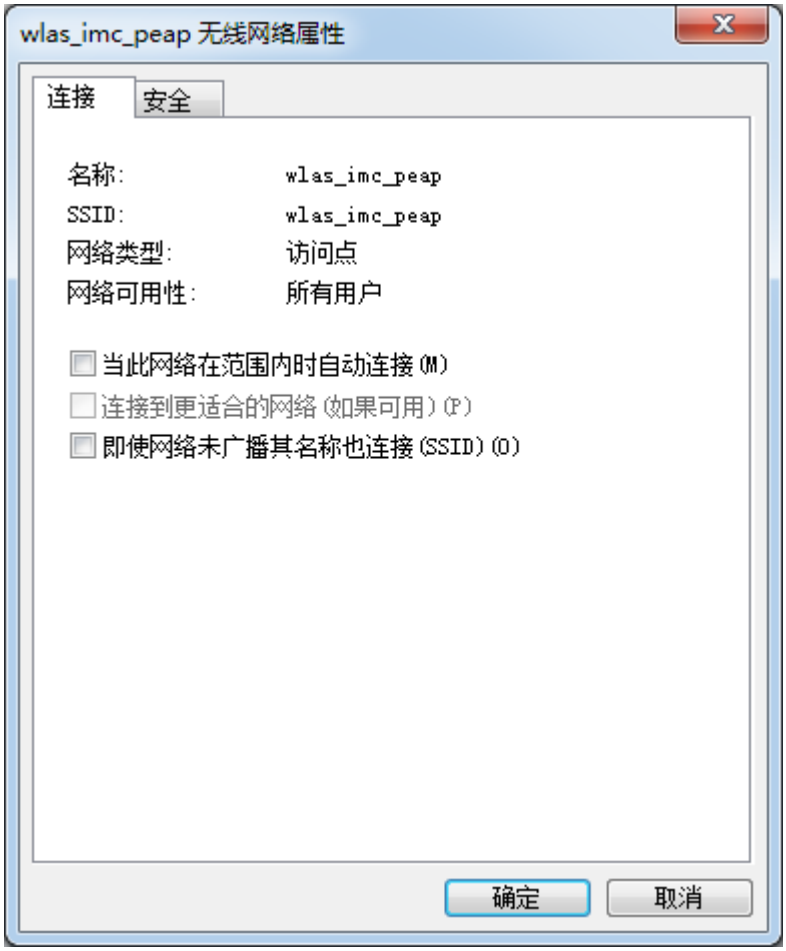


图1-12 无线网卡配置过程

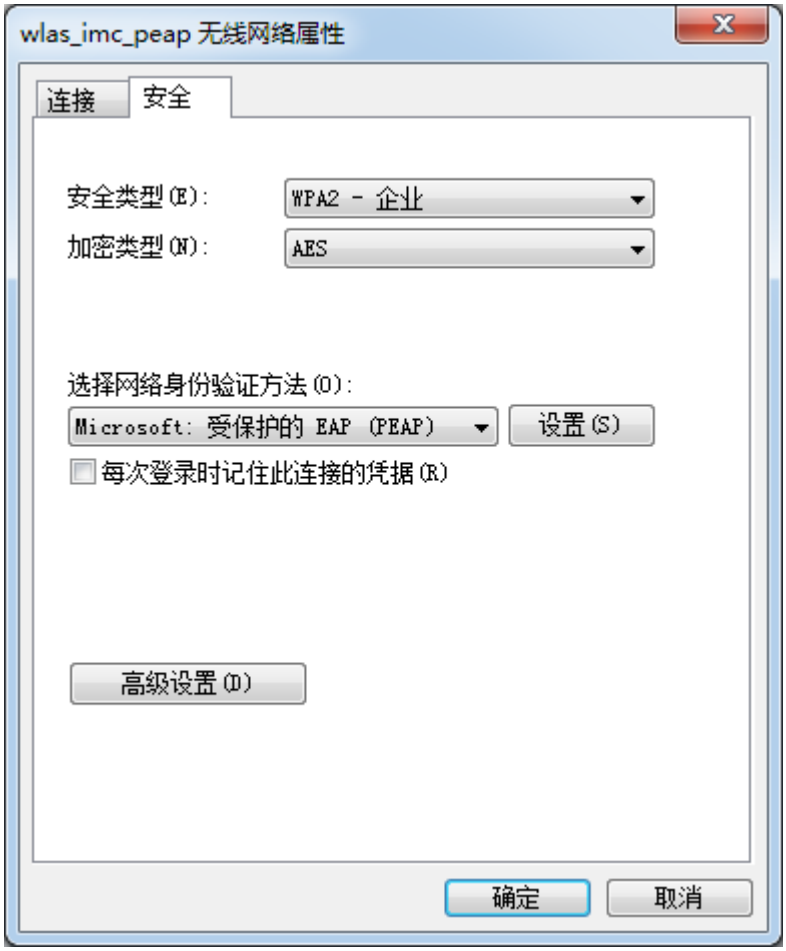


图1-13 无线网卡配置过程

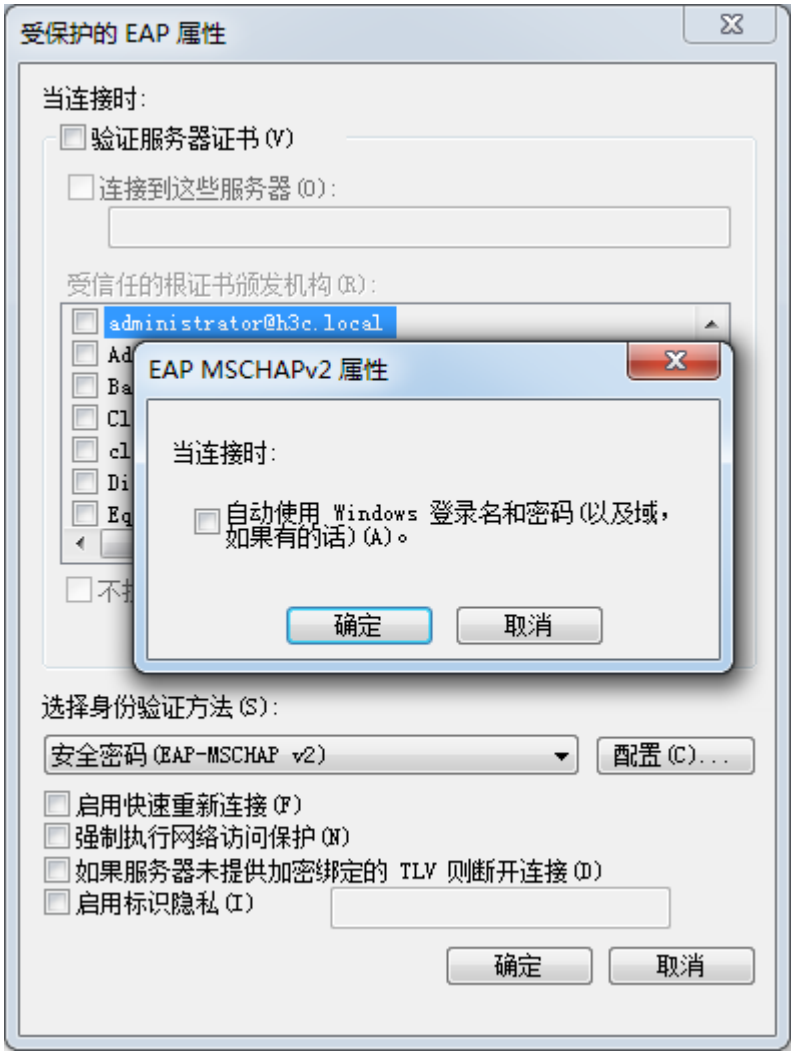


图1-14 无线网卡配置过程

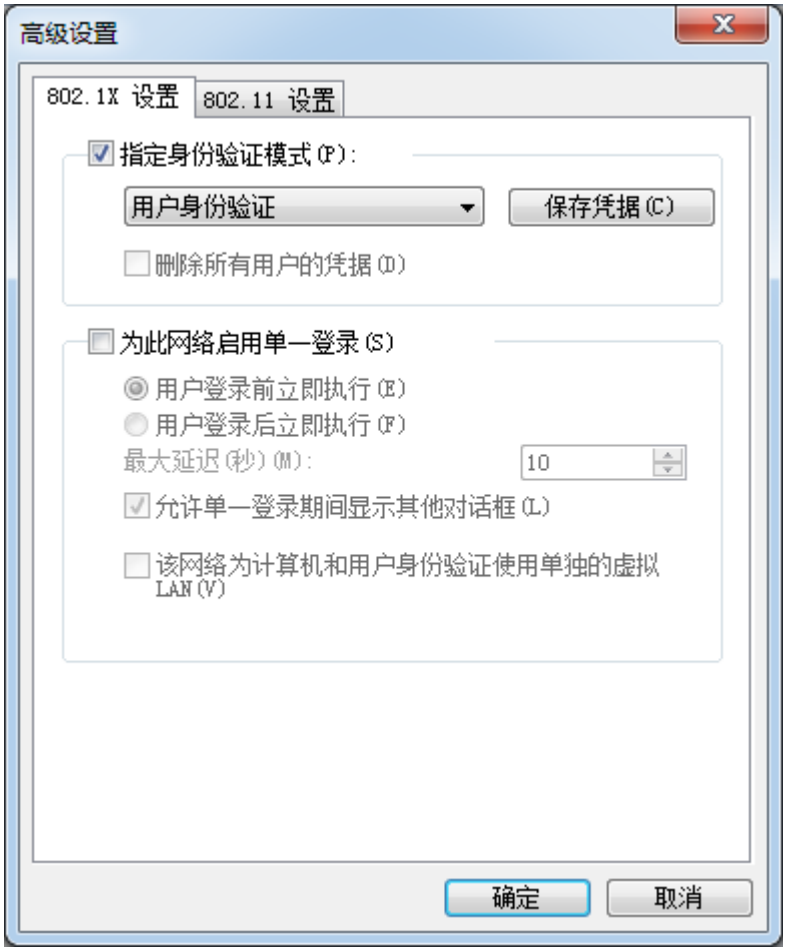
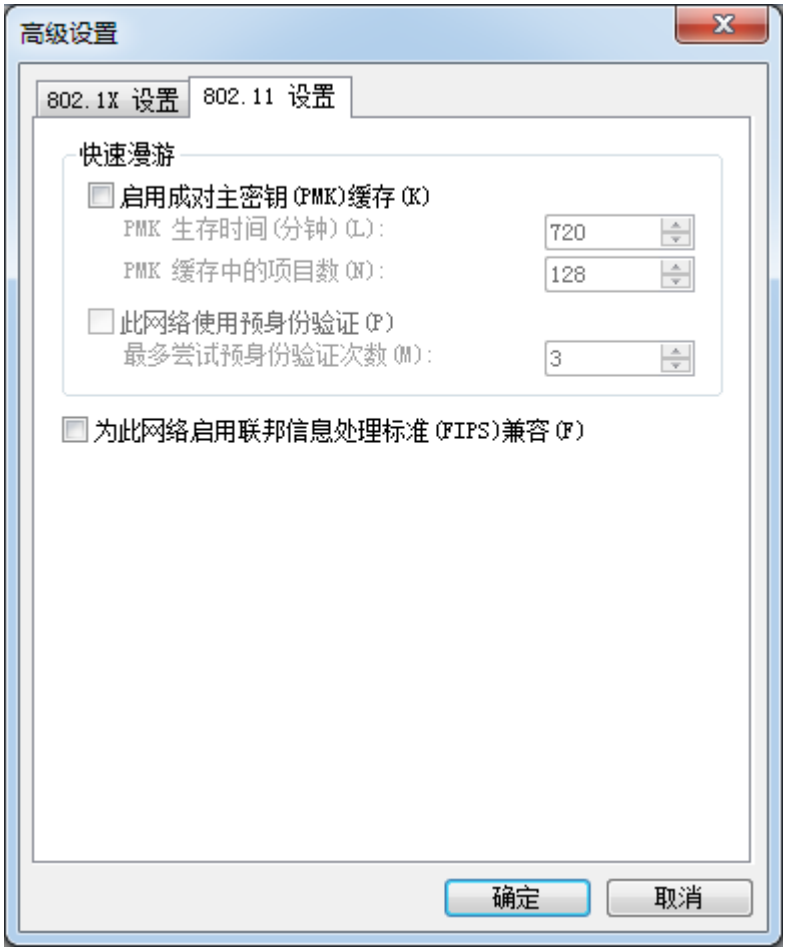


图1-15 无线网卡配置过程



4. 验证结果

客户端通过 802.1X 认证成功关联 AP，并且可以访问无线网络。

- 通过 **display dot1x connection** 命令显示 802.1X 用户连接信息，可以看到用户名和客户端输入的用户名一致。

```
[AP] display dot1x connection
User MAC address           : 0023-8933-2090
BSSID                      : 000f-e201-0003
User name                  : user
Authentication domain      : imc
Authentication method      : EAP
Initial VLAN               : 1
Authorization VLAN         : N/A
Authorization ACL number   : N/A
Authorization user profile : N/A
Termination action         : Default
Session timeout period     : 6001 s
Online from                : 2014/04/18 09:25:18
Online duration            : 0h 1m 1s
```

```
Total connections: 1.
```

- 通过 display wlan client 显示命令查看无线客户端在线情况查看 802.1X 用户上线信息，可看到 802.1X 用户成功上线。

```
[AP] display wlan client
Total number of clients           : 1

MAC address    Username   AP name     RID   IP address      IPv6 address   VLAN
0023-8933-2090 user       ap          1     10.18.1.100                    1
```

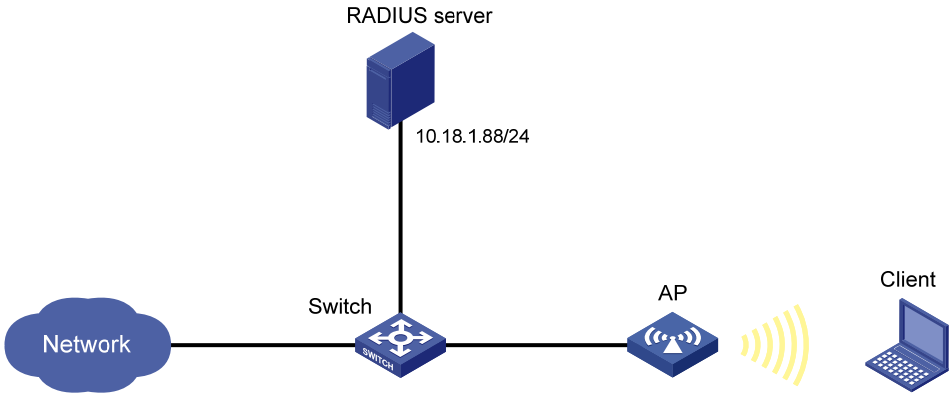
1.7.3 使用RADIUS服务器进行MAC地址认证典型配置举例

1. 组网需求

- AP 和 RADIUS 服务器通过交换机建立连接，RADIUS 服务器的 IP 地址为 10.18.1.88。
- 要求使用远程 MAC 认证认证方式进行用户身份认证。

2. 组网图

图1-16 使用 RADIUS 服务器进行 MAC 地址认证典型配置组网图



3. 配置步骤

说明

确保 RADIUS 服务器与设备路由可达，完成服务器的配置，并成功添加了接入用户账户：用户名为：123，密码为 dot1x。

(1) 配置 RADIUS 方案

配置 RADIUS 方案，名称为 imcc，认证服务器的 IP 地址为 10.18.1.88，端口号为 1812，配置计费服务器的 IP 地址为 10.18.1.88，端口号为 1813，认证密钥为明文 12345678，计费密钥为明文 12345678，用户名格式为 without-domain。

```
<AP> system-view
[AP] radius scheme imcc
[AP-radius-imcc] primary authentication 10.18.1.88 1812
[AP-radius-imcc] primary accounting 10.18.1.88 1813
```

```
[AP-radius-imcc] key authentication simple 12345678
[AP-radius-imcc] key accounting simple 12345678
[AP-radius-imcc] user-name-format without-domain
[AP-radius-imcc] quit
```

(2) 配置 ISP 域的 AAA 方法

配置名称为 imc 的 ISP 域，并将认证、授权和计费的方式配置为使用 RADIUS 方案 imcc。

```
[AP] domain imc
[AP-isp-imc] authentication lan-access radius-scheme imcc
[AP-isp-imc] authorization lan-access radius-scheme imcc
[AP-isp-imc] accounting lan-access radius-scheme imcc
[AP-isp-imc] quit
```

(3) 配置 MAC 地址认证

配置 MAC 地址认证用户名格式为固定用户名格式，用户名为 123，密码为明文 dot1x（若配置成大写、不带连字符的 mac 地址格式，服务器需要配置与之对应的用户名格式；若配置成固定用户名格式，服务器也需要配置与其对应的用户名格式）。

```
[AP] mac-authentication user-name-format fixed account 123 password simple dot1x
```

配置无线服务模板 maca_imc 的 SSID 为 maca_imc，并设置用户认证方式为 MAC 地址认证，ISP 域为 imc。

```
[AP] wlan service-template maca_imc
[AP-wlan-st-maca_imc] ssid maca_imc
[AP-wlan-st-maca_imc] client-security authentication-mode mac
[AP-wlan-st-maca_imc] mac-authentication domain imc
```

无线服务模板使能。

```
[AP-wlan-st-maca_imc] service-template enable
[AP-wlan-st-maca_imc] quit
```

(4) 将无线服务模板绑定到 WLAN-Radio 1/0/1 接口上

```
[AP] interface wlan-radio 1/0/1
[AP-WLAN-Radio1/0/1] undo shutdown
[AP-WLAN-Radio1/0/1] service template maca_imc
[AP-WLAN-Radio1/0/1] quit
```

(5) 配置 RADIUS server（iMC V7）

 说明

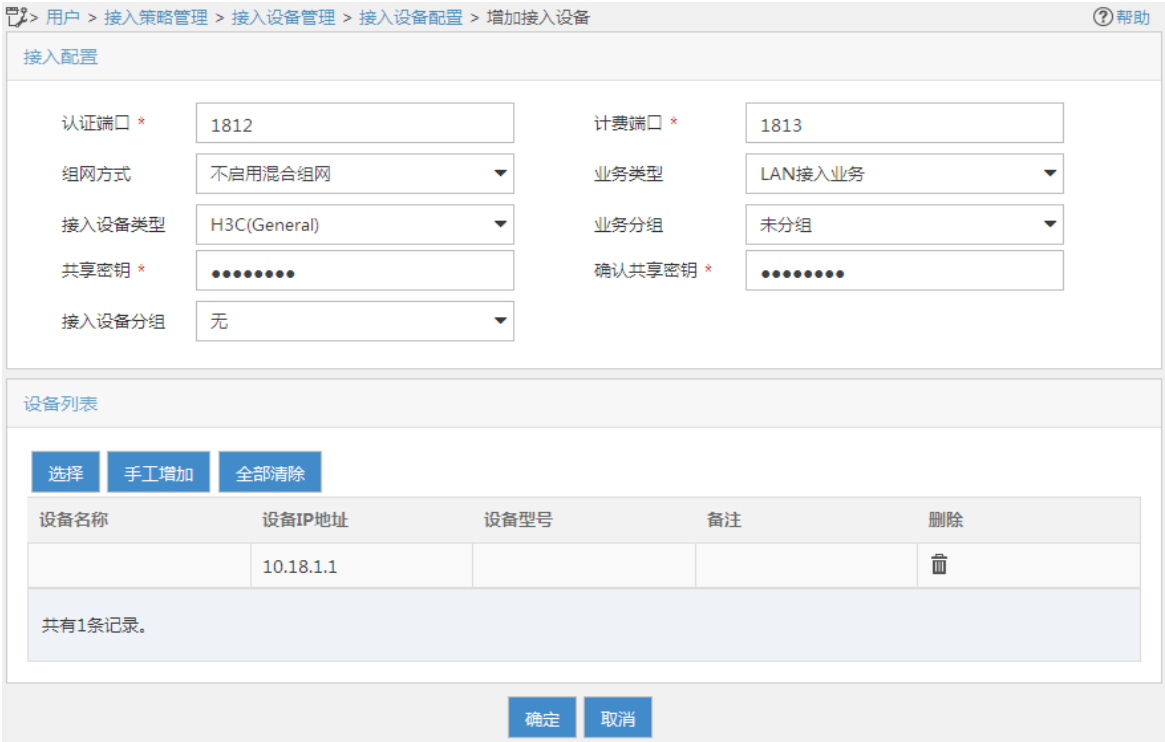
下面以 iMC 为例（使用 iMC 版本为：iMC PLAT 7.1、iMC UAM 7.1），说明 RADIUS server 的基本配置。

增加接入设备。

登录进入 iMC 管理平台，选择“用户”页签，单击导航树中的[接入策略管理/接入设备管理/接入设备配置]菜单项，进入接入设备配置页面，在该页面中单击“增加”按钮，进入增加接入设备页面。

- 设置认证、计费共享密钥为 12345678，其它保持缺省配置；
- 选择或手工增加接入设备，添加 IP 地址为 10.18.1.1 的接入设备。

图1-17 增加接入设备页面

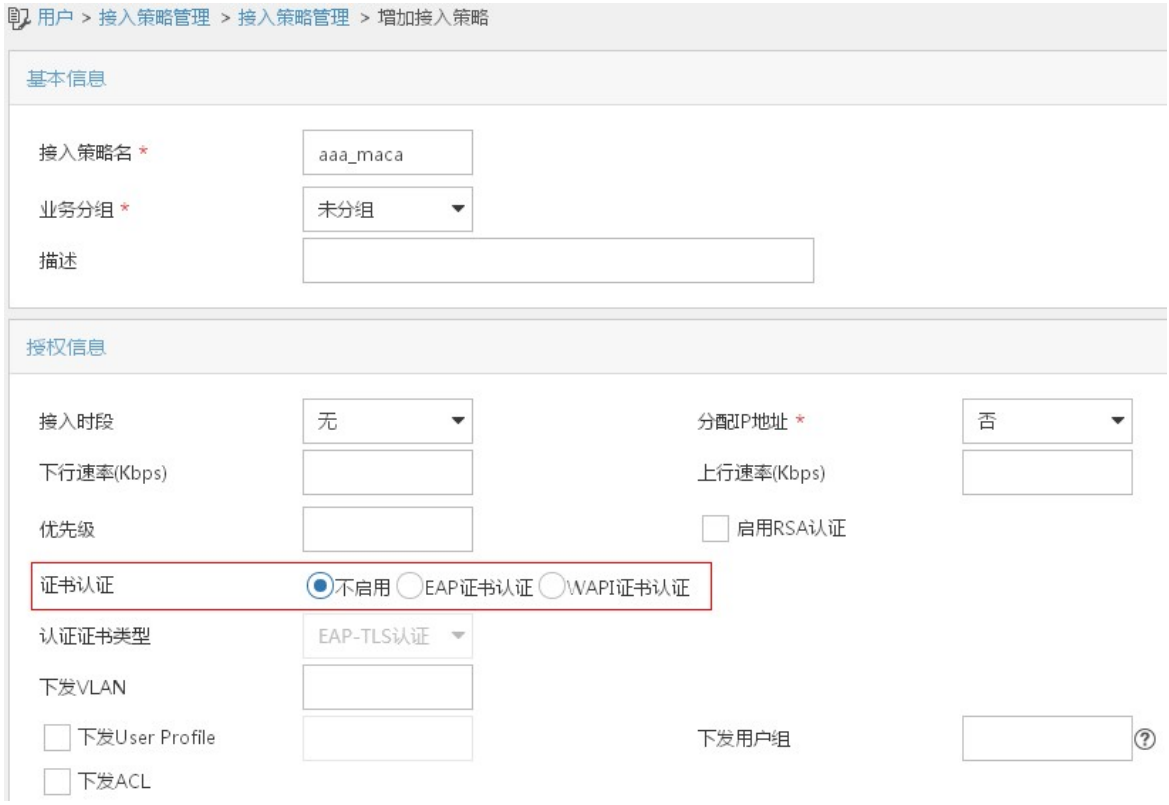


增加服务策略。

选择“用户”页签，单击导航树中的[接入策略管理/接入策略管理]菜单项，进入接入策略管理页面，在该页面中单击“增加”按钮，进入增加接入策略页面。

- 设置接入策略名为 dot1x；
- 选择认证证书类型为 EAP-PEAP 认证，认证证书子类型为 MS-CHAPV2 认证。认证证书子类型需要与客户端的身份验证方法一致。

图1-18 增加服务策略页面



增加接入服务。

选择“用户”页签，单击导航栏中的[接入策略管理/接入服务管理]菜单项，进入接入服务管理页面，在该页面中单击<增加>按钮，进入增加接入服务页面。

- 设置服务名为 dot1x；
- 设置缺省接入策略为已经创建的 dot1x 策略。

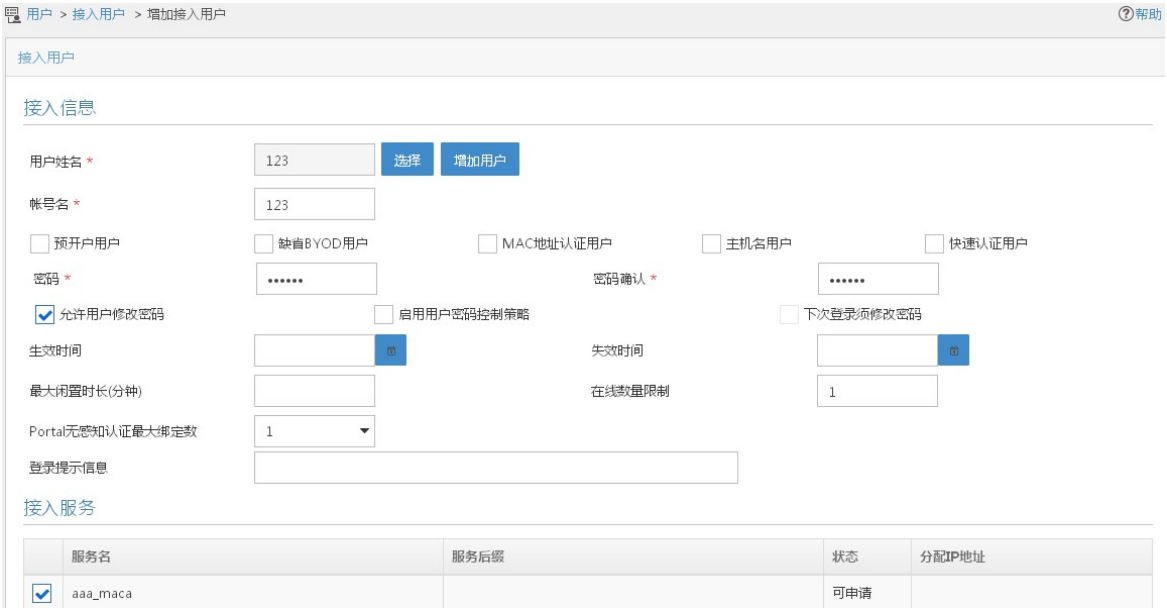
图1-19 增加接入服务页面

增加接入用户。

选择“用户”页签，单击导航树中的[接入用户管理/接入用户]菜单项，进入接入用户页面，在该页面中单击<增加>按钮，进入增加接入用户页面。

- 添加用户 user；
- 添加帐号名为 user，密码为 dot1x；
- 选中刚才配置的服务 dot1x。

图1-20 增加接入用户页面



4. 验证结果

客户端通过 MAC 认证成功关联 AP，并且可以访问无线网络。

- 通过 **display mac-authentication connection** 命令显示 MAC 用户连接信息。

```
[AP] display mac-authentication connection
User MAC address              : 0023-8933-2098
BSSID                         : 000f-e201-0001
User name                     : 123
Authentication domain         : imc
Initial VLAN                  : 1
Authorization VLAN            : N/A
Authorization ACL number      : N/A
Authorization user profile    : N/A
Termination action            : Radius-Request
Session timeout period        : 6001 s
Online from                   : 2014/04/17 17:21:12
Online duration               : 0h 0m 30s

Total connections: 1.
```

- 通过 **display wlan client** 显示命令查看无线客户端在线情况查看 MAC 地址认证用户上线信息，可看到 MAC 地址认证用户成功上线。

```
[AP] display wlan client
Total number of clients          : 1
```

MAC address	Username	AP name	RID	IP address	IPv6 address	VLAN
0023-8933-2098	123	ap	1	10.18.1.100		1