# 目 录

# 1 包过滤

## 1.1 概述

包过滤是指采用 ACL 规则对接口、VLAN 或全局入方向或出方向的报文进行过滤，即对匹配上 ACL 规则的报文按照其中定义的匹配动作允许或拒绝通过，对未匹配上任何 ACL 规则的报文则按照指定的缺省动作进行处理。

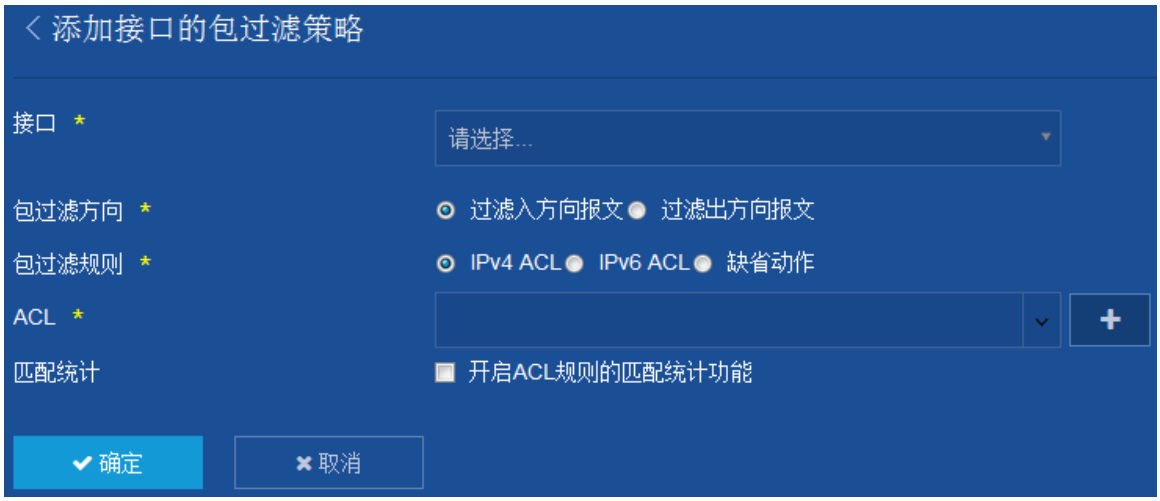
## 1.2 配置接口包过滤

(1) 在导航栏中选择“安全 > 包过滤”，默认进入“接口”页签的页面，如下图所示。

图1-1 包过滤


(2) 单击  ，设置接口的包过滤策略，如下图所示。

图1-2 接口的包过滤策略




(3) 配置接口的包过滤策略，详细参数说明如下表所示。

(4) 单击<确定>按钮完成操作。

表1-1 包过滤策略详细说明

| 标题项 | 说明 |
| --- | --- |
| 接口 | 选择下拉框设置接口 |
| 包过滤方向 | 设置包过滤的方向，包括过滤入方向报文和过滤出方向报文 |
| 包过滤规则 | 设置包过滤的规则，包括IPv4 ACL、IPv6 ACL和缺省动作 |
| ACL | 添加ACL |
| 匹配统计 | 用于统计基于硬件应用的ACL规则匹配次数<br>开启该功能后，系统对ACL规则匹配情况进行统计 |

## 1.3 配置VLAN包过滤

(1) 在导航栏中选择“安全 > 包过滤”，默认进入“接口”页签的页面。

(2) 单击“VLAN”页签，如下图所示。

图1-3 包过滤

(3) 单击，设置 VLAN 的包过滤策略，如下图所示。

图1-4 VLAN 的包过滤策略


(4) 配置 VLAN 的包过滤策略，详细参数说明如下表所示。

(5) 单击<确定>按钮完成操作。

表1-2 包过滤策略详细说明

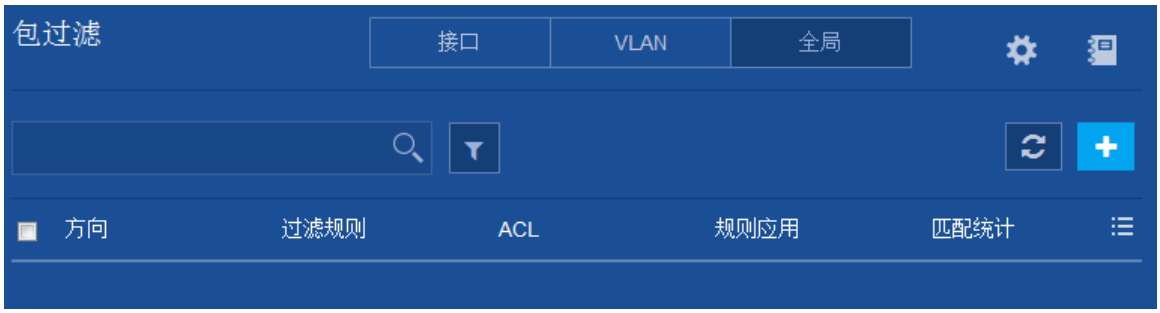
| 标题项 | 说明 |
| --- | --- |
| VLAN | 输入VLAN ID |
| 包过滤方向 | 设置包过滤方向，包括过滤入方向报文和过滤出方向报文 |
| 包过滤规则 | 设置包过滤的规则，包括IPv4 ACL、IPv6 ACL和缺省动作 |
| ACL | 添加ACL |
| 匹配统计 | 用于统计基于硬件应用的ACL规则匹配次数<br>开启该功能后，系统对ACL规则匹配情况进行统计 |

## 1.4 配置全局包过滤

(1) 在导航栏中选择“安全 > 包过滤”，默认进入“接口”页签的页面。

(2) 单击“全局”页签，如下图所示。

图1-5 包过滤




(3) 单击，设置全局包过滤策略，如下图所示。

图1-6 全局包过滤策略


(4) 配置全局包过滤策略，详细参数说明如下表所示。

(5) 单击<确定>按钮完成操作。

表1-3 包过滤策略详细说明

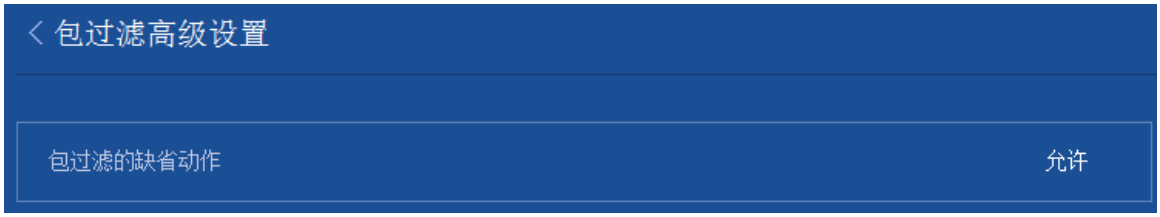
| 标题项 | 说明 |
| --- | --- |
| 包过滤方向 | 设置包过滤方向，包括过滤入方向报文和过滤出方向报文 |
| 包过滤规则 | 设置包过滤的规则，包括IPv4 ACL、IPv6 ACL和缺省动作 |
| ACL | 添加ACL |
| 匹配统计 | 用于统计基于硬件应用的ACL规则匹配次数<br>开启该功能后，系统对ACL规则匹配情况进行统计 |

## 1.5 配置包过滤高级信息

(1) 在导航栏中选择“安全 > 包过滤”，默认进入“接口”页签的页面。

(2) 单击  ，进入包过滤高级设置页面，如下图所示。

图1-7 包过滤




(3) 单击“包过滤的缺省动作”后的参数，如下图所示。

图1-8 包过滤高级设置


(4) 配置包过滤的缺省动作，可选择“允许未匹配上 ACL 规则的报文通过”或“禁止未匹配上 ACL 规则的报文通过”。

(5) 单击<确定>按钮完成操作。

# 2 IP Source Guard

## 2.1 概述

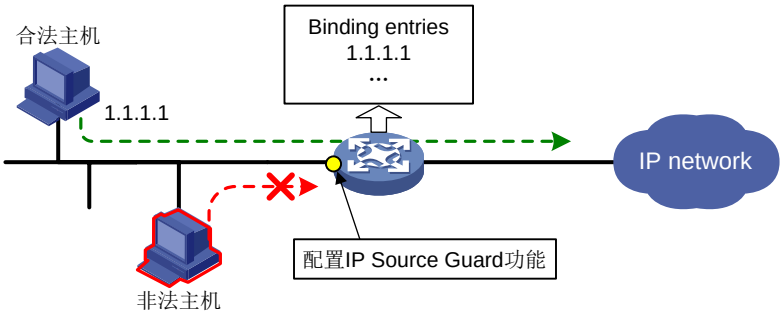
IP Source Guard 功能用于对接口收到的报文进行过滤控制，通常配置在接入用户侧的接口上，以防止非法用户报文通过，从而限制了对网络资源的非法使用（比如非法主机仿冒合法用户 IP 接入网络），提高了接口的安全性。

如图 2-1 所示，配置了 IP Source Guard 功能的接口接收到用户报文后，首先查找与该接口绑定的表项（简称为绑定表项），如果报文的信息与某绑定表项匹配，则转发该报文，否则丢弃该报文。IP Source Guard 可以根据报文的源 IP 地址、源 MAC 地址对报文进行过滤。报文的这些特征项可单独或组合起来与接口进行绑定，形成如下几类绑定表项：

- IP 绑定表项
- MAC 绑定表项
- IP＋MAC 绑定表项
- IP＋VLAN 绑定表项
- MAC＋VLAN 绑定表项
- IP＋MAC＋VLAN 绑定表项

IP Source Guard 绑定表项可以通过手工配置和动态获取两种方式生成。

图2-1 IP Source Guard 功能示意图




说明

IP Source Guard 的绑定功能是针对接口的，一个接口配置了绑定功能后，仅对该接口接收的报文进行限制，其它接口不受影响。

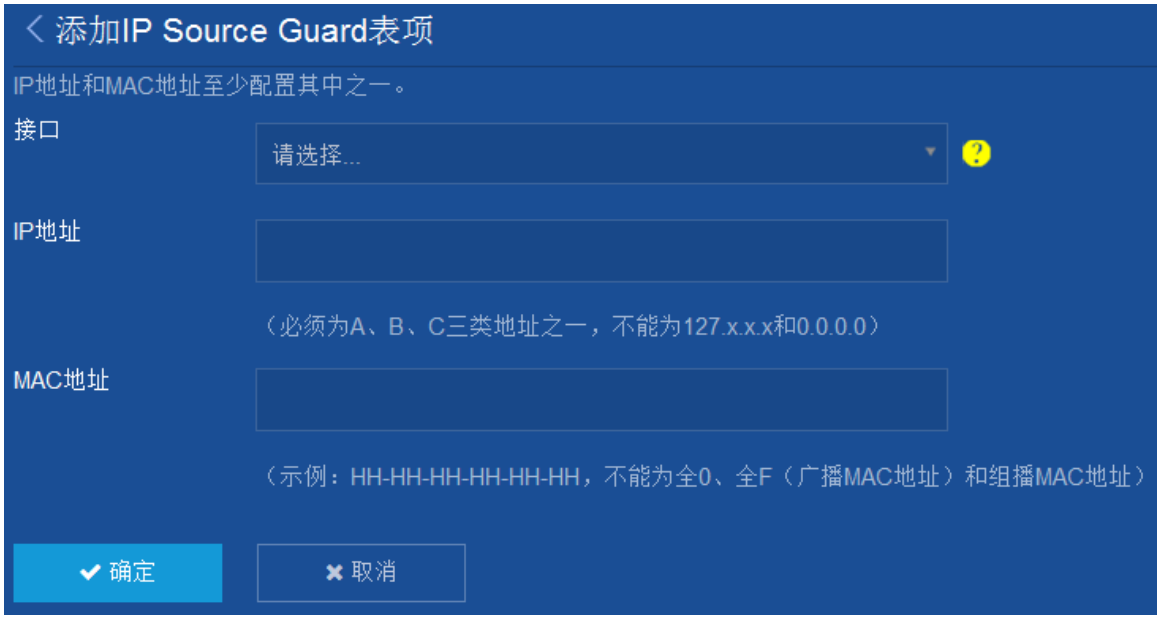
## 2.2 配置IP Source Guard

(1) 在导航栏中选择“安全 > IP Source Guard”，进入“IP Source Guard”页面，如下图所示。

图2-2 IP Source Guard


(2) 单击  ，设置 IP Source Guard 表项，如下图所示。

图2-3 添加 IP Source Guard 表项




(3) 根据需要配置参数，详细参数说明如下表所示。

(4) 单击<确定>按钮完成操作。

表2-1 IP Source Guard 表项参数说明

| 标题项 | 说明 |
| --- | --- |
| 接口 | 选择下拉框设置接口 |

| 标题项 | 说明 |
| --- | --- |
| IP地址 | 设置合法主机的 IP 地址，即与交换机端口相连接的设备（一般是 PC）的 IP 地址 |
| MAC地址 | 设置合法主机的MAC地址 |

# 3 802.1X

说明

本章节主要描述了 802.1X 的相关概念及配置步骤。由于通过配置端口安全特性也可以为用户提供 802.1X 认证服务，且还可以提供 802.1X 和 MAC 地址认证的扩展和组合应用，因此在需要灵活使用以上两种认证方式的组网环境下，推荐使用端口安全特性。无特殊组网要求的情况下，无线环境中通常使用端口安全特性。而在仅需要 802.1X 特性来完成接入控制的组网环境下，推荐单独使用 802.1X 特性。关于端口安全特性的详细介绍和具体配置请参见“端口安全”。

## 3.1 概述

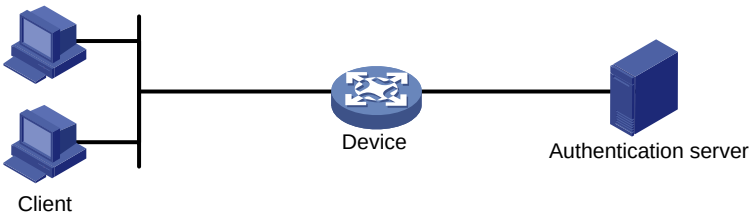
最初，IEEE 802 LAN/WAN 委员会为解决无线局域网网络安全问题，提出了 802.1X 协议。后来，802.1X 协议作为局域网的一个普通接入控制机制在以太网中被广泛应用，主要解决以太网内认证和安全方面的问题。

802.1X 协议是一种基于端口的网络接入控制协议，即在局域网接入设备的端口上对所接入的用户设备进行认证，以便用户设备控制对网络资源的访问。

### 3.1.1 802.1X 的体系结构

802.1X 系统中包括三个实体：客户端（Client）、设备端（Device）和认证服务器（Authentication server），如下图所示。

图3-1 802.1X 体系结构图




- 客户端是请求接入局域网的用户终端设备，它由局域网中的设备端对其进行认证。客户端上必须安装支持 802.1X 认证的客户端软件。
- 设备端是局域网中控制客户端接入的网络设备，位于客户端和认证服务器之间，为客户端提供接入局域网的端口（物理端口或逻辑端口），并通过与服务器的交互来对所连接的客户端进行认证。

- 认证服务器用于对客户端进行认证、授权和计费，通常为 RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）服务器。认证服务器根据设备端发送来的客户端认证信息来验证客户端的合法性，并将验证结果通知给设备端，由设备端决定是否允许客户端接入。在一些规模较小的网络环境中，认证服务器的角色也可以由设备端来代替，即由设备端对客户端进行本地认证、授权和计费。

### 3.1.2 802.1X 对端口的控制

#### 1. 受控/非受控端口

设备端为客户端提供接入局域网的端口被划分为两个逻辑端口：受控端口和非受控端口。任何到达该端口的帧，在受控端口与非受控端口上均可见。

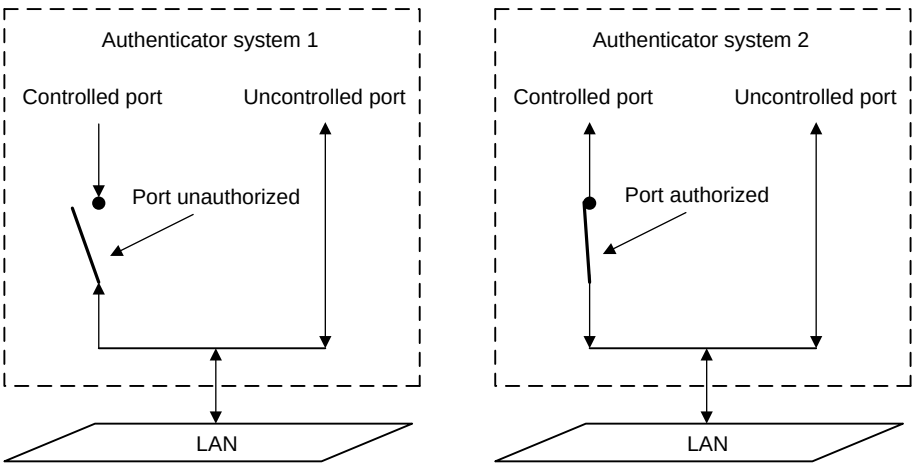
- 非受控端口始终处于双向连通状态，主要用来传递 EAPOL（Extensible Authentication Protocol over LAN，局域网上的可扩展认证协议）协议帧，保证客户端始终能够发出或接收认证报文。
- 受控端口在授权状态下处于双向连通状态，用于传递业务报文；在非授权状态下禁止从客户端接收任何报文。

#### 2. 授权/非授权状态

设备端利用认证服务器对需要接入局域网的客户端执行认证，并根据认证结果（Accept 或 Reject）对受控端口的授权状态进行相应地控制。

下图显示了受控端口上不同的授权状态对通过该端口报文的影响。图中对比了两个 802.1X 认证系统的端口状态。系统 1 的受控端口处于非授权状态，不允许报文通过；系统 2 的受控端口处于授权状态，允许报文通过。

图3-2 受控端口上授权状态的影响




#### 3. 受控方向

在非授权状态下，受控端口可以被设置成单向受控和双向受控。

- 处于双向受控状态时，禁止帧的发送和接收；
- 处于单向受控状态时，禁止从客户端接收帧，但允许向客户端发送帧。

说明

目前，设备上的受控端口只能处于单向受控状态。

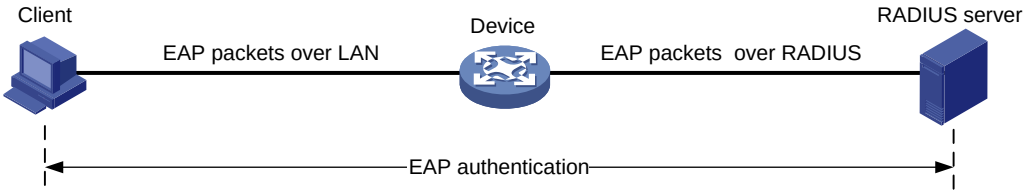
### 3.1.3 802.1X 认证报文的交互机制

802.1X 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互。EAP 是一种 C/S 模式的认证框架，它可以支持多种认证方法，例如 MD5-Challenge、EAP-TLS、PEAP 等。在客户端与设备端之间，EAP 报文使用 EAPOL 封装格式承载于数据帧中传递。在设备端与 RADIUS 服务器之间，EAP 报文的交互有以下两种处理机制。

#### 1. EAP 中继

设备对收到的 EAP 报文进行中继，使用 EAPOR（EAP over RADIUS）封装格式将其承载于 RADIUS 报文中发送给 RADIUS 服务器进行认证。

图3-3 EAP 中继原理示意图

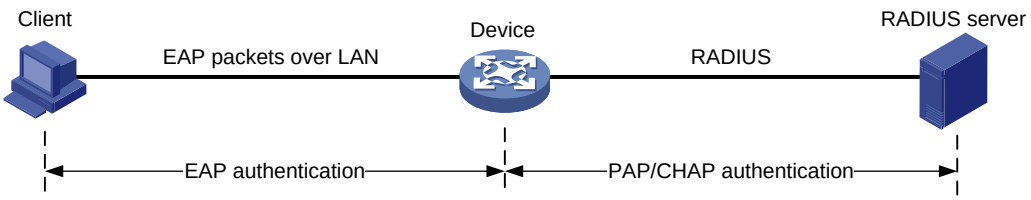



该处理机制下，EAP 认证过程在客户端和 RADIUS 服务器之间进行，RADIUS 服务器作为 EAP 服务器来处理客户端的 EAP 认证请求，设备相当于一个代理，仅对 EAP 报文做中转，因此设备处理简单，并能够支持 EAP 的各种认证方法，但要求 RADIUS 服务器支持相应的 EAP 认证方法。

#### 2. EAP 终结

设备对 EAP 认证过程进行终结，将收到的 EAP 报文中的客户端认证信息封装在标准的 RADIUS 报文中，与服务器之间采用 PAP（Password Authentication Protocol，密码验证协议）或 CHAP（Challenge Handshake Authentication Protocol，质询握手验证协议）方法进行认证。

图3-4 EAP 终结原理示意图




该处理机制下，由于现有的 RADIUS 服务器基本均可支持 PAP 认证和 CHAP 认证，因此对服务器无特殊要求，但设备处理较为复杂，它需要作为 EAP 服务器来解析与处理客户端的 EAP 报文，且目前仅能支持 MD5-Challenge 类型的 EAP 认证以及 iNode 802.1X 客户端发起的“用户名+密码”方式的 EAP 认证。

说明

如果客户端采用了 MD5-Challenge 类型的 EAP 认证，则设备端只能采用 CHAP 认证；如果 iNode 802.1X 客户端采用了“用户名+密码”方式的 EAP 认证，设备上可选择使用 PAP 认证或 CHAP 认证，从安全性上考虑，通常使用 CHAP 认证。

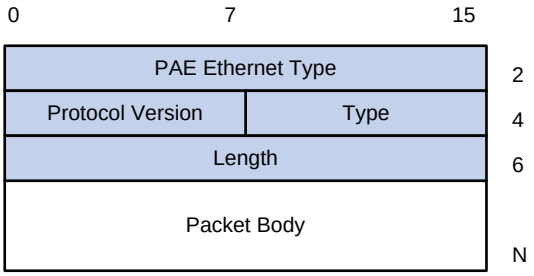
### 3.1.4 EAP 报文的封装

#### 1. EAPOL 数据帧的封装

(1) EAPOL 数据帧的格式

EAPOL 是 802.1X 协议定义的一种承载 EAP 报文的封装格式，主要用于在局域网中传送客户端和设备端之间的 EAP 协议报文。EAPOL 数据包的格式如下图所示。

图3-5 EAPOL 数据包格式




- PAE Ethernet Type：表示协议类型。EAPOL 的协议类型为 0x888E。
- Protocol Version：表示 EAPOL 数据帧的发送方所支持的 EAPOL 协议版本号。
- Type：表示 EAPOL 数据帧类型。目前设备上支持的 EAPOL 数据帧类型如下表所示。

表3-1 EAPOL 数据帧类型

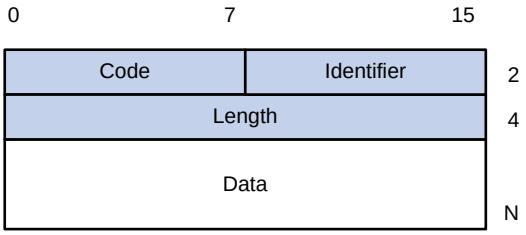
| 类型值 | 数据帧类型 | 说明 |
|---|---|---|
| 0x00 | EAP-Packet | 认证信息帧，用于承载客户端和设备端之间的EAP报文<br>• 在终结方式下，该帧中的客户端认证信息会被设备端重新封装并承载于 RADIUS 报文中发送给认证服务器<br>• 在中继方式下，该帧承载的 EAP 报文会被设备端直接封装在 RADIUS 报文的 EAP 属性中发送给认证服务器 |
| 0x01 | EAPOL-Start | 认证发起帧，用于客户端向设备端发起认证请求 |
| 0x02 | EAPOL-Logoff | 退出请求帧，用于客户端向设备端发起下线请求 |

- Length：表示数据域的长度，也就是 Packet Body 字段的长度，单位为字节。当 EAPOL 数据帧的类型为 EAPOL-Start 或 EAPOL-Logoff 时，该字段值为 0，表示后面没有 Packet Body 字段。
- Packet Body：数据域的内容。

(2) EAP 报文的格式

当 EAPOL 数据帧的类型为 EAP-Packet 时，Packet Body 字段的内容就是一个 EAP 报文，格式如下图所示。

图3-6 EAP 报文格式




- Code：EAP 报文的类型，包括 Request（1）、Response（2）、Success（3）和 Failure（4）。
- Identifier：用于匹配 Request 消息和 Response 消息的标识符。
- Length：EAP 报文的长度，包含 Code、Identifier、Length 和 Data 域，单位为字节。
- Data：EAP 报文的内容，该字段仅在 EAP 报文的类型为 Request 和 Response 时存在，它由类型域和类型数据两部分组成，例如，类型域为 1 表示 Identity 类型，类型域为 4 表示 MD5 Challenge 类型。

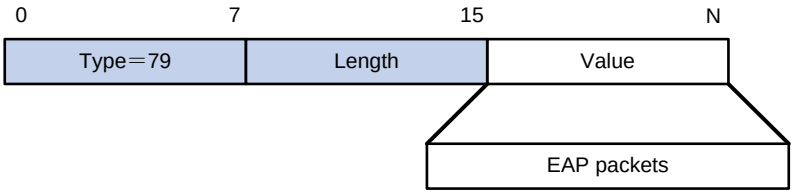
### 2. EAP 报文在 RADIUS 中的封装

RADIUS 为支持 EAP 认证增加了两个属性：EAP-Message（EAP 消息）和 Message-Authenticator（消息认证码）。在含有 EAP-Message 属性的数据包中，必须同时包含 Message-Authenticator 属性。关于 RADIUS 报文格式的介绍请参见“RADIUS”。

(1) EAP-Message

如下图所示，EAP-Message 属性用来封装 EAP 报文，Value 域最长 253 字节，如果 EAP 报文长度大于 253 字节，可以对其进行分片，依次封装在多个 EAP-Message 属性中。

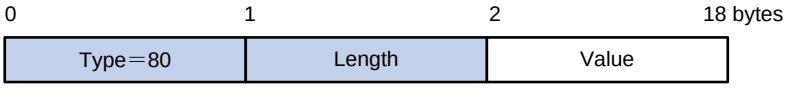
图3-7 EAP-Message 属性封装




(2) Message-Authenticator

如下图所示，Message-Authenticator 属性用于在 EAP 认证过程中验证携带了 EAP-Message 属性的 RADIUS 报文的完整性，避免报文被窜改。如果接收端对接收到的 RADIUS 报文计算出的完整性校验值与报文中携带的 Message-Authenticator 属性的 Value 值不一致，该报文会被认为无效而丢弃。

图3-8 Message-Authenticator 属性封装




### 3.1.5 802.1X 的认证触发方式

802.1X 的认证过程可以由客户端主动发起，也可以由设备端发起。

#### 1. 客户端主动触发方式

- 组播触发：客户端主动向设备端发送 EAPOL-Start 报文来触发认证，该报文目的地址为组播 MAC 地址 01-80-C2-00-00-03。
- 广播触发：客户端主动向设备端发送 EAPOL-Start 报文来触发认证，该报文的目的地址为广播 MAC 地址。该方式可解决由于网络中有些设备不支持上述的组播报文，而造成认证设备无法收到客户端认证请求的问题。

---

说明

目前，iNode 的 802.1X 客户端可支持广播触发方式。

---

#### 2. 设备端主动触发方式

设备端主动触发方式用于支持不能主动发送 EAPOL-Start 报文的客户端，例如 Windows XP 自带的 802.1X 客户端。设备主动触发认证的方式分为以下两种：

- 组播触发：设备每隔 N 秒（缺省为 30 秒）主动向客户端组播发送 Identity 类型的 EAP-Request 帧来触发认证。
- 单播触发：当设备收到源 MAC 地址未知的报文时，主动向该 MAC 地址单播发送 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。

### 3.1.6 802.1X 的认证过程

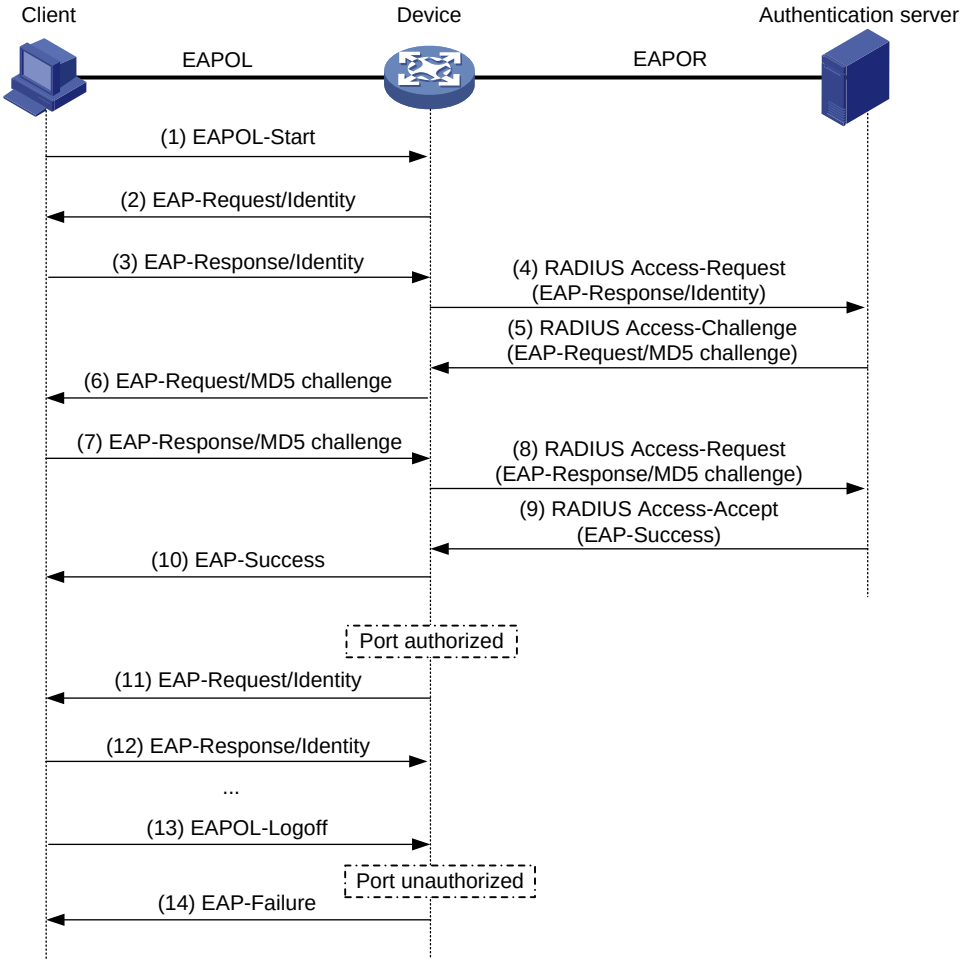
802.1X 系统支持采用 EAP 中继方式和 EAP 终结方式与远端 RADIUS 服务器交互。以下关于两种认证方式的过程描述，都以客户端主动发起认证为例。

#### 1. EAP 中继方式

这种方式是 IEEE 802.1X 标准规定的，将 EAP 承载在其它高层协议中，如 EAP over RADIUS，以便扩展认证协议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，分别用来封装 EAP 报文及对携带 EAP-Message 的 RADIUS 报文进行保护。

下面以 MD5-Challenge 认证方法为例介绍基本业务流程，认证过程如下图所示。

图3-9 IEEE 802.1X 认证系统的 EAP 中继方式业务流程




(2) 当用户需要访问外部网络时打开 802.1X 客户端程序，输入已经申请、登记过的用户名和密码，发起连接请求。此时，客户端程序将向设备端发出认证请求帧（EAPOL-Start），开始启动一次认证过程。

(3) 设备端收到认证请求帧后，将发出一个 Identity 类型的请求帧（EAP-Request/Identity）要求用户的客户端程序发送输入的用户名。

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

(5) 设备端将客户端发送的响应帧中的 EAP 报文封装在 RADIUS 报文（RADIUS Access-Request）中发送给认证服务器进行处理。

(6) RADIUS 服务器收到设备端转发的用户名信息后，将该信息与数据库中的用户名列表中对比，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 报文发送给设备端。

(7) 设备端将 RADIUS 服务器发送的 MD5 Challenge 转发给客户端。

(8) 客户端收到由设备端传来的 MD5 Challenge 后，用该 Challenge 对密码部分进行加密处理，生成 EAP-Response/MD5 Challenge 报文，并发送给设备端。

(9) 设备端将此 EAP-Response/MD5 Challenge 报文封装在 RADIUS 报文（RADIUS Access-Request）中发送给 RADIUS 认证服务器。

(10) 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，并向设备端发送认证通过报文（RADIUS Access-Accept）。

(11) 设备收到认证通过报文后向客户端发送认证成功帧（EAP-Success），并将端口改为授权状态，允许用户通过端口访问网络。

(12) 用户在线期间，设备端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。

(13) 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，设备端就会让用户下线，防止用户因为异常原因下线而设备无法感知。

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

(15) 设备端把端口状态从授权状态改变成未授权状态，并向客户端发送 EAP-Failure 报文。

---

说明

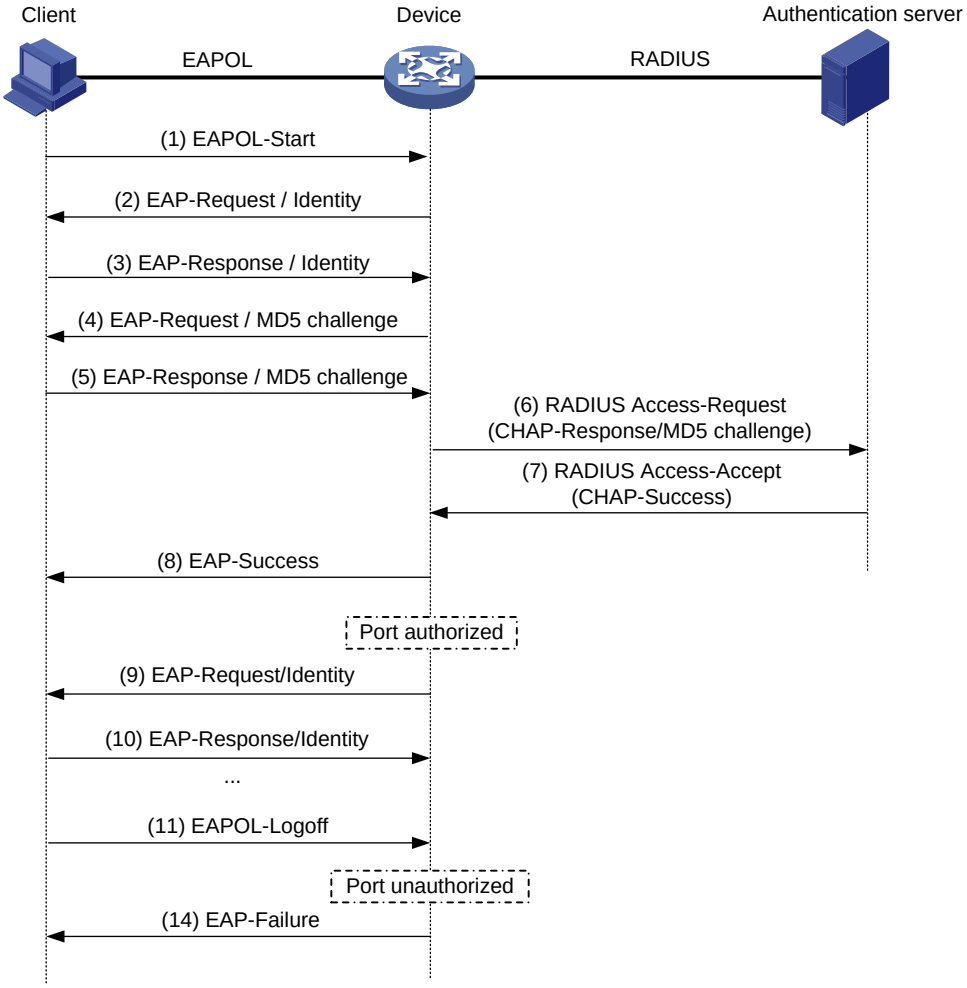
EAP 中继方式下，需要保证在客户端和 RADIUS 服务器上选择一致的 EAP 认证方法，而在设备上，只需要配置 802.1X 用户的认证方式为 EAP 即可。

---

### 2. EAP 终结方式

这种方式将 EAP 报文在设备端终结并映射到 RADIUS 报文中，利用标准 RADIUS 协议完成认证、授权和计费。设备端与 RADIUS 服务器之间可以采用 PAP 或者 CHAP 认证方法。下面以 CHAP 认证方法为例介绍基本业务流程，如下图所示。

图3-10 IEEE 802.1X 认证系统的 EAP 终结方式业务流程




EAP 终结方式与 EAP 中继方式的认证流程相比，不同之处在于步骤(4)中用来对用户密码信息进行加密处理的 MD5 Challenge 由设备端生成，之后设备端会把用户名、MD5 Challenge 和客户端加密后的密码信息一起送给 RADIUS 服务器，进行相关的认证处理。

### 3.1.7 802.1X 的接入控制方式

设备不仅支持协议所规定的基于端口的接入认证方式（Port Based），还对其进行了扩展、优化，支持基于 MAC 的接入控制方式（MAC Based）。

- 当采用基于端口的接入控制方式时，只要该端口下的第一个用户认证成功后，其它接入用户无须认证就可使用网络资源，但是当第一个用户下线后，其它用户也会被拒绝使用网络。
- 采用基于 MAC 的接入控制方式时，该端口下的所有接入用户均需要单独认证，当某个用户下线时，也只有该用户无法使用网络。

### 3.1.8 802.1X 扩展功能

#### 1. 支持 VLAN 下发

802.1X 用户在服务器上通过认证时，服务器会把授权信息传送给设备端。如果服务器上指定了授权给该用户的下发 VLAN，则服务器发送给设备的授权信息中将含有下发的 VLAN 信息，设备根据用户认证上线的端口连接类型，按以下三种情况将端口加入下发 VLAN 中。

表3-2 不同类型的端口加入下发的 VLAN

| 接入控制方式 | Access 端口 | Trunk 端口 | Hybrid 端口 |
|---|---|---|---|
| Port Based | 端口离开用户配置的VLAN，加入下发的VLAN | 端口允许下发的VLAN通过，并且将缺省VLAN修改为下发的VLAN | 端口允许下发的VLAN以不携带Tag的方式通过，并且将缺省VLAN修改为下发的VLAN |
| MAC Based | 端口离开用户配置的VLAN，加入第一个通过认证的用户的下发VLAN | 端口允许下发的VLAN通过，并且将缺省VLAN修改为第一个通过认证的用户的下发VLAN | 端口允许下发的VLAN以不携带Tag的方式通过<br>• 若端口上启用了 MAC VLAN 功能，则根据下发的 VLAN 动态地创建基于用户 MAC 的 VLAN，而端口的缺省 VLAN ID 并不改变<br>• 若端口上未启用 MAC VLAN 功能，则端口的缺省 VLAN ID 修改为第一个通过认证的用户的下发 VLAN 的 VLAN ID |
| | 说明：只有启用了MAC VLAN功能的端口上才允许给不同的用户MAC下发不同的VLAN。其它情况下，下发给所有用户的VLAN必须相同，否则仅第一个通过认证的用户的可以认证成功。 | | |

下发的 VLAN 并不影响端口的配置。但是，下发的 VLAN 的优先级高于用户配置的 VLAN，即通过认证后起作用的 VLAN 是下发的 VLAN，用户配置的 VLAN 在用户下线后生效。

说明

- 对于 Hybrid 端口，不建议把服务器将要下发或已经下发的 VLAN 配置为携带 Tag 的方式加入端口。
- 在启动了 802.1X 周期性重认证功能的 Hybrid 端口上，若用户在 MAC VLAN 功能开启之前上线，则 MAC VLAN 功能不能对该用户生效，即系统不会根据服务器下发的 VLAN 生成该用户的 MAC VLAN 表项，只有该在线用户重认证成功且服务器下发的 VLAN 发生变化时，MAC VLAN 功能才会对它生效。

#### 2. Guest VLAN

Guest VLAN 功能允许用户在未认证的情况下，访问某一特定 VLAN 中的资源。这个特定的 VLAN 称之为 Guest VLAN，该 VLAN 内通常放置一些用于用户下载客户端软件或其他升级程序的服务器。根据端口的接入控制方式不同，Guest VLAN 的生效情况有所不同。

(1) 端口的接入控制方式为 Port Based

在接入控制方式为 Port Based 的端口上配置 Guest VLAN 后，若在一定的时间内（默认 90 秒），该端口上无客户端进行认证，则该端口将被加入 Guest VLAN，所有在该端口接入的用户将被授权访问 Guest VLAN 里的资源。不同链路类型的端口加入 Guest VLAN 的情况有所不同，具体情况与端口加入服务器下发的 VLAN 类似，请参见“1. 支持 VLAN 下发”。

当端口上处于 Guest VLAN 中的用户发起认证且失败时：如果端口配置了认证失败 VLAN，则该端口会被加入认证失败 VLAN；如果端口未配置认证失败 VLAN，则该端口仍然处于 Guest VLAN 内。关于认证失败 VLAN 的具体介绍请参见“3. 认证失败 VLAN”。

当端口上处于 Guest VLAN 中的用户发起认证且成功时，端口会离开 Guest VLAN，之后端口加入 VLAN 情况与认证服务器是否下发 VLAN 有关，具体如下：

- 若认证服务器下发 VLAN，则端口加入下发的 VLAN 中。用户下线后，端口离开下发的 VLAN 回到初始 VLAN 中，该初始 VLAN 为端口加入 Guest VLAN 之前所在的 VLAN。
- 若认证服务器不下发 VLAN，则端口回到初始 VLAN 中。用户下线后，端口仍在该初始 VLAN 中。

(2) 端口的接入控制方式为 MAC Based

在接入控制方式为 MAC Based 的端口上配置 Guest VLAN 后，端口上未认证的用户被授权访问 Guest VLAN 里的资源。

当端口上处于 Guest VLAN 中的用户发起认证且失败时，如果端口配置了认证失败 VLAN，则认证失败的用户将被加入认证失败 VLAN；如果端口未配置认证失败 VLAN，则该用户将仍然处于 Guest VLAN 内。

当端口上处于 Guest VLAN 中的用户发起认证且成功时，设备会根据认证服务器是否下发 VLAN 决定将该用户加入到下发的 VLAN 中，或回到加入 Guest VLAN 之前端口所在的初始 VLAN。

### 3. 认证失败 VLAN

认证失败 VLAN（Auth-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 称之为认证失败 VLAN。需要注意的是，这里的认证失败是认证服务器因某种原因明确拒绝用户认证通过，比如用户密码错误，而不是认证超时或网络连接等原因造成的认证失败。

根据端口的接入控制方式不同，认证失败 VLAN 的生效情况有所不同。

(1) 端口的接入控制方式为 Port Based

在接入控制方式为 Port Based 的端口上配置认证失败 VLAN 后，若该端口上有用户认证失败，则该端口会被加入到认证失败 VLAN，所有在该端口接入的用户将被授权访问认证失败 VLAN 里的资源。端口加入认证失败 VLAN 的情况与加入授权下发 VLAN 相同，与端口链路类型有关。

当加入认证失败 VLAN 的端口上有用户发起认证并失败，则该端口将会仍然处于认证失败 VLAN 内；如果认证成功，则该端口会离开认证失败 VLAN，之后端口加入 VLAN 情况与认证服务器是否下发 VLAN 有关，具体如下：

- 若认证服务器下发 VLAN，则端口加入下发的 VLAN 中。用户下线后，端口会离开下发的 VLAN 回到初始 VLAN 中，该初始 VLAN 为端口加入认证失败 VLAN 之前所在的 VLAN。
- 若认证服务器未下发 VLAN，则端口回到初始 VLAN 中。用户下线后，端口仍在该初始 VLAN 中。

(2) 端口的接入控制方式为 MAC Based

在接入控制方式为 MAC Based 的端口上配置认证失败 VLAN 后，该端口上认证失败的用户将被授权访问认证失败 VLAN 里的资源。

当认证失败 VLAN 中的用户再次发起认证时，如果认证成功，则设备会根据认证服务器是否下发 VLAN 决定将该用户加入到下发的 VLAN 中，或回到加入认证失败 VLAN 之前端口所在的初始 VLAN；如果认证失败，则该用户仍然留在该 VLAN 中。

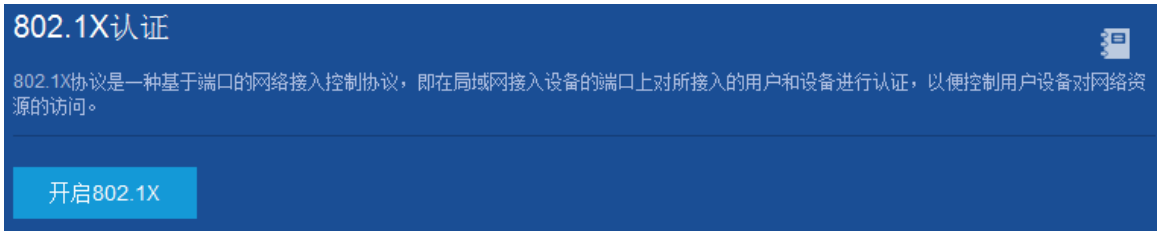
#### 4. 支持 ACL 下发

802.1X 支持 ACL（Access Control List，访问控制列表）下发功能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 服务器上指定了要下发给该用户的授权 ACL，则设备会根据服务器下发的授权 ACL 对用户所在端口的数据流进行过滤，仅允许 ACL 规则中允许的数据流通过该端口。由于服务器上指定的是授权 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服务器的授权 ACL 设置或设备上对应的 ACL 规则来改变用户的访问权限。

## 3.2 开启802.1X功能

(1) 在导航栏中选择“安全 > 802.1X”，进入“802.1X 认证”页面，如下图所示。

图3-11 开启 802.1X 认证




(2) 单击“开启 802.1X”，开启 802.1X 认证功能，进入如下图所示页面。

说明

单击，可关闭 802.1X 认证功能。

图3-12 802.1X 认证


(3) 选择端口对应的“开启 802.1X”下的复选框，开启对应端口的 802.1X 功能。

(4) 设置最大用户数。

(5) 单击<确定>按钮完成操作。

## 3.3 配置802.1X的高级信息

(1) 单击  可进行 802.1X 高级设置，如下图所示。

图3-13 802.1X 高级设置


(2) 根据需要配置参数，详细参数说明请参见下表。

(3) 单击“确定”完成操作。

表3-3 802.1X 高级设置参数说明

| 标题项 | 说明 |
| --- | --- |
| 认证方法 | 设置认证方法，可选CHAP、PAP和EAP |
| 域名分隔符 | 802.1X 支持的域名分隔符，可选@、\、/和. |
| 周期性重认证时间间隔 | 设备根据该时间间隔定期向该端口在线用户发起重认证，以检测用户连接变化、确保用户的正常在线，并及时更新服务器下发的授权属性 |
| 周期发送握手请求报文时间间隔 | 设备根据该时间间隔定期向在线用户发送握手请求报文，以检测用户的在线情况 |
| 重发服务器认证请求报文时间间隔 | 设置重发服务器认证请求报文的时间间隔 |

| 标题项 | 说明 |
| --- | --- |
| 重发客户端EAP-Request/MD5 Challenge请求报文时间间隔 | 设置重发客户端EAP-Request/MD5 Challenge请求报文的时间间隔 |
| 重发客户端EAP-Request/Identity请求报文时间间隔 | 设置重发客户端EAP-Request/Identity请求报文的时间间隔 |
| 向接入用户发送认证请求报文的最大次数 | 设备向用户重发该认证请求报文后，若设备连续发送认证请求报文的次数达到该值，仍然没有得到用户响应，则停止发送认证请求 |
| SmartOn | 在开始802.1X认证请求前增加了SmartOn认证，如果SmartOn认证不成功，则不再继续进行802.1X认证 |
| EAD快速部署 | 显示EAD快速部署的ON/OFF状态 |

# 4 MAC 地址认证

## 4.1 概述

### 4.1.1 MAC 地址认证简介

MAC 地址认证是一种基于端口和 MAC 地址对用户的网络访问权限进行控制的认证方法，它不需要用户安装任何客户端软件。设备在启动了 MAC 地址认证的端口上首次检测到用户的 MAC 地址以后，即启动对该用户的认证操作。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，则允许其通过端口访问网络资源，否则该用户的 MAC 地址就被添加为静默 MAC。在静默时间内（可通过静默定时器配置），来自此 MAC 地址的用户报文到达时，设备直接做丢弃处理，以防止非法 MAC 短时间内的重复认证。

注意

若配置的静态 MAC 或者当前认证通过的 MAC 地址与静默 MAC 相同，则 MAC 地址认证失败后的 MAC 静默功能将会失效。

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。
- 在接入设备上进行本地认证。

目前，MAC 地址认证支持两种类型的用户名格式：

- MAC 地址用户名：使用用户的 MAC 地址作为认证时的用户名和密码。
- 固定用户名：不论用户的 MAC 地址为何值，所有用户均使用在设备上预先配置的用户名和密码进行认证。由于同一个端口下可以有多个用户进行认证，因此这种情况下端口上的所有 MAC 地址认证用户均使用同一个固定用户名进行认证。

### 4.1.2 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：

- 采用 MAC 地址用户名时，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。
- 采用固定用户名时，设备将已经在本地配置的用户名和密码作为待认证用户的用户名和密码，发送给 RADIUS 服务器。

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。

### 4.1.3 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：

- 采用 MAC 地址用户名时，需要配置的本地用户名和密码为各接入用户的 MAC 地址。
- 采用固定用户名时，需要配置的本地用户名为自定义的，所有用户对应的用户名和密码与自定义的一致。

### 4.1.4 MAC 地址认证定时器

MAC 地址认证过程受以下定时器的控制：

- 离线检测定时器：用来设置设备用户空闲超时的时间间隔。如果在两个时间间隔之内，没有来自用户的流量通过，设备将切断用户的连接，同时通知 RADIUS 服务器，停止对该用户的计费。
- 静默定时器：用来设置用户认证失败以后，设备停止对其提供认证服务的时间间隔。在静默期间，设备不对来自该用户的报文进行认证处理，直接丢弃。静默期后，如果设备再次收到该用户的报文，则依然可以对其进行认证处理。
- 认证超时定时器：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，如果认证超时定时器超时时设备一直没有收到 RADIUS 服务器的应答，则设备将在相应的端口上禁止此用户访问网络。

### 4.1.5 和 MAC 地址认证配合使用的特性

#### 1. 下发 VLAN

为了将受限的网络资源与未认证用户隔离，通常将受限的网络资源和用户划分到不同的 VLAN。MAC 地址认证支持认证服务器授权下发 VLAN 功能，即当用户通过 MAC 地址认证后，认证服务器支持将指定的受限网络资源所在的 VLAN 作为授权 VLAN 下发到用户认证的端口。该端口被加入到授权 VLAN 中后，用户便可以访问这些受限的网络资源。

#### 2. 下发 ACL

从认证服务器下发的 ACL 被称为授权 ACL，它为用户访问网络提供了良好的过滤条件设置功能。MAC 地址认证支持认证服务器授权下发 ACL 功能，即当用户通过 MAC 地址认证后，如果 RADIUS 服务器上配置了授权 ACL，则设备会根据服务器下发的授权 ACL 对用户所在端口的数据流进行控制。为使下发的授权 ACL 生效，需要提前在设备上配置相应的 ACL 规则。而且在用户访问网络的过程中，可以通过改变服务器的授权 ACL 设置来改变用户的访问权限。

#### 3. 认证失败 VLAN

认证失败 VLAN（Auth-Fail VLAN）功能允许用户在认证失败的情况下可以访问某一特定 VLAN 中的资源，比如获取客户端软件，升级客户端或执行其他一些用户升级程序。这个 VLAN 称之为认证失败 VLAN。需要注意的是，这里的认证失败是认证服务器因某种原因明确拒绝用户认证通过，比如用户密码错误，而不是认证超时或网络连接等原因造成的认证失败。

如果接入用户的端口上配置了认证失败 VLAN，则该端口上认证失败的用户会被加入认证失败 VLAN，即该用户被授权访问认证失败 VLAN 里的资源。若认证失败 VLAN 中的用户再次发起认证未成功，则该用户将仍然处于认证失败 VLAN 内；若认证成功，则会根据认证服务器是否下发 VLAN 将用户加入到下发的 VLAN 中，或回到加入认证失败 VLAN 之前端口所在的 VLAN。

## 4.2 配置MAC地址认证

通过使用 MAC 地址认证，可以对用户的网络访问权限进行控制。

### 4.2.1 配置准备

- 关闭全局的端口安全功能。
- 创建并配置 ISP 域。
- 若采用本地认证方式，需要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 地址认证用户账号。

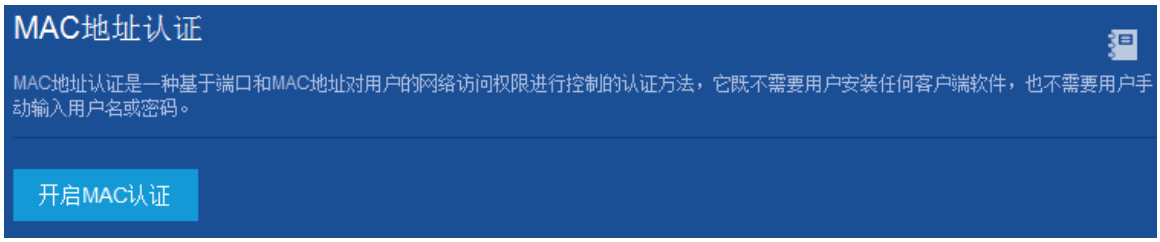
注意

创建本地用户或添加远程用户账号时，需要注意这些用户的用户名必须与设备上指定的 MAC 地址认证用户名格式保持一致。

### 4.2.2 开启 MAC 地址认证功能

(1) 在导航栏中选择“安全 > MAC 地址认证”，进入“MAC 地址认证”页面，如下图所示。

图4-1 开启 MAC 地址认证




(2) 单击“开启 MAC 认证”，开启 MAC 地址认证功能，进入如下图所示页面。

说明

单击，可关闭 MAC 地址认证功能。

图4-2 MAC 地址认证


(3) 选择端口对应的“开启 MAC 地址认证”下的复选框。

(4) 设置最大用户数。

(5) 单击<确定>按钮完成操作。

### 4.2.3 查看静默 MAC 信息

(1) 在导航栏中选择“安全 > MAC 地址认证”，默认进入“MAC 地址认证”页签的页面。

(2) 单击“静默 MAC 信息”页签，如下图所示。可查看静默 MAC 地址的信息，包括 MAC、所在 VLAN 以及接口。

图4-3 静默 MAC 信息

### 4.2.4 配置 MAC 地址认证的高级信息

(1) 在导航栏中选择“安全 > MAC 地址认证”，默认进入“MAC 地址认证”页签的页面，如下图所示。

图4-4 MAC 地址认证


(2) 单击  ，可进行 MAC 地址认证高级设置，进入如下图所示页面。

图4-5 MAC 地址认证高级设置


(3) 根据需要设置参数，详细参数说明如下表所示。

(4) 单击<确定>按钮完成操作。

表4-1 MAC 地址认证高级设置

| 标题项 | 说明 |
| --- | --- |
| 用户名格式 | 设置用户名的格式，包括如下：<br>• MAC 地址用户格式：使用用户的 MAC 地址作为认证时的用户名和密码<br>• 固定用户名格式：不论用户的 MAC 地址为何值，所有用户均使用设备上指定的一个固定用户名和密码替代用户的 MAC 地址作为身份信息进行认证 |
| 用户认证域 | 设备支持指定 MAC 地址认证用户使用的认证域，可以通过两种方式实现：<br>• 在全局配置中指定一个认证域，该认证域对所有开启了 MAC 地址认证的端口生效<br>• 在接口配置中指定该端口的认证域，不同的端口可以指定不同的认证域 |
| 用户下线检测时间间隔 | 用来设置用户空闲超时的时间间隔 |
| 静默时间间隔 | 设置静默时间间隔 |
| 服务器超时时间间隔 | 设置服务器超时时间间隔 |

# 4.3 MAC地址认证典型配置举例

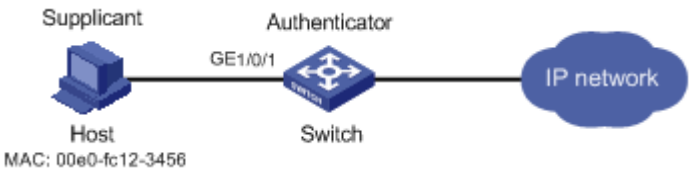
## 4.3.1 MAC 地址认证典型配置举例

### 1. 组网需求

如下图所示，某用户的工作站与交换机的端口 GigabitEthernet1/01 相连接。

- 管理者希望在交换机的各端口上对用户接入进行 MAC 地址认证，以控制其对 Internet 的访问。
- 要求设备每隔 180 秒就对用户是否下线进行检测；并且当用户认证失败时，需等待 3 分钟后才能对用户再次发起认证。
- 所有用户都属于域：aabbcc.net，认证时使用本地认证的方式。使用用户的源 MAC 地址做用户名和密码。

图4-6 MAC 地址认证配置组网图




### 2. 配置步骤

(1) 配置本地接入用户，用户名和密码均为接入用户的 MAC 地址“00-e0-fc-12-34-56”，可用服务为“LAN 接入”。详细请参见“10.2.1 配置本地用户”。

(2) 创建 ISP 域。

步骤 1：在导航栏中选择“安全 > ISP 域”。

步骤 2：单击  。

步骤 3：配置 ISP 域信息，如下图所示。

- 输入域名为“aabbcc.net”。
- 接入方式为“LAN 接入”。
- 选择认证为“本地认证”。

步骤 4：单击<确定>按钮完成操作。

图4-7 创建 ISP 域


(3) 配置全局的 MAC 地址认证。

步骤 1：在导航栏中选择“安全 > MAC 地址认证”。

步骤 2：单击  。

步骤 3：进行如下配置，如下图所示。

- 选择用户名类型为“MAC 地址用户格式”。
- 选择用户认证域为“aabbcc.net”。

- 输入用户下线检测时间间隔为“180”。
- 输入静默时间间隔为“180”。

步骤 3：单击<确定>按钮完成操作。

图4-8 配置全局的 MAC 地址认证

(4) 启用端口 GigabitEthernet1/0/1 的 MAC 地址认证。

步骤 1：在导航栏中选择“安全 > MAC 地址认证”，默认进入“MAC 地址认证”页签的页面。

步骤 2：选择端口 GigabitEthernet1/0/1 对应的“开启 MAC 地址认证”下的复选框，如下图所示。

步骤 3：单击<确定>按钮完成操作。

图4-9 启用端口 GigabitEthernet1/0/1 的 MAC 地址认证

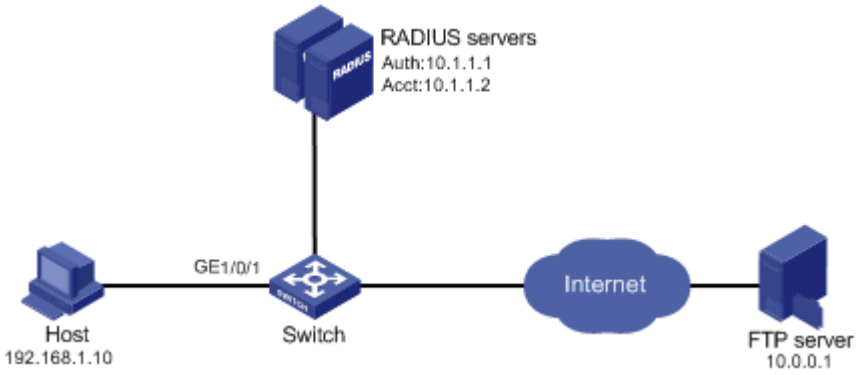

## 4.3.2 下发 ACL 典型配置举例

### 1. 组网需求

如下图所示，主机 Host 通过 MAC 地址认证接入网络，认证服务器为 RADIUS 服务器。Internet 网络中有一台 FTP 服务器，IP 地址为 10.0.0.1。

- 认证时使用用户的源 MAC 地址做用户名和密码。
- 在认证服务器上配置授权下发 ACL 3000。
- 在 Switch 的 GigabitEthernet1/0/1 上开启 MAC 地址认证，并配置 ACL 3000。
- 当用户认证成功上线，认证服务器下发 ACL 3000。此时 ACL 3000 在 GigabitEthernet1/0/1 上生效，Host 可以访问 Internet，但不能访问 FTP 服务器。

图4-10 下发 ACL 典型配置组网图




## 2. 配置步骤

说明

- 确保 RADIUS 服务器与 Switch 路由可达。
- 由于该例中使用了 MAC 地址认证的缺省用户名和密码，即使用用户的源 MAC 地址做用户名与密码，因此还要保证 RADIUS 服务器上正确添加了接入用户的用户名和密码。
- 指定 RADIUS 服务器上的授权 ACL 为设备上配置的 ACL 3000。

(1) 配置 RADIUS 方案 system。

步骤 1：在导航栏中选择“安全 > RADIUS”，进入 RADIUS 的配置页面。

步骤 2：单击，进入新建 RADIUS 方案的配置页面。

步骤 3：进行如下配置，如下图所示。

- 输入方案名称为“system”。
- 在“认证服务器”的“主服务器”区域，进行如下配置：
  - 选择类型为“IP 地址”。
  - 输入 IP 地址/FQDN 为“10.1.1.1”。
  - 输入端口为“1812”。
  - 输入共享密钥为“expert”。
  - 选择状态为“活动”。
- 在“计费服务器”的“主服务器”区域，进行如下配置：
  - 选择类型为“IP 地址”。
  - 输入 IP 地址/FQDN 为“10.1.1.2”。
  - 输入端口为“1813”。
  - 输入共享密钥为“expert”。
  - 选择状态为“活动”。

步骤 4：单击<确定>按钮完成操作。

图4-11 添加 RADIUS 方案 system


(2) 添加 ISP 域。

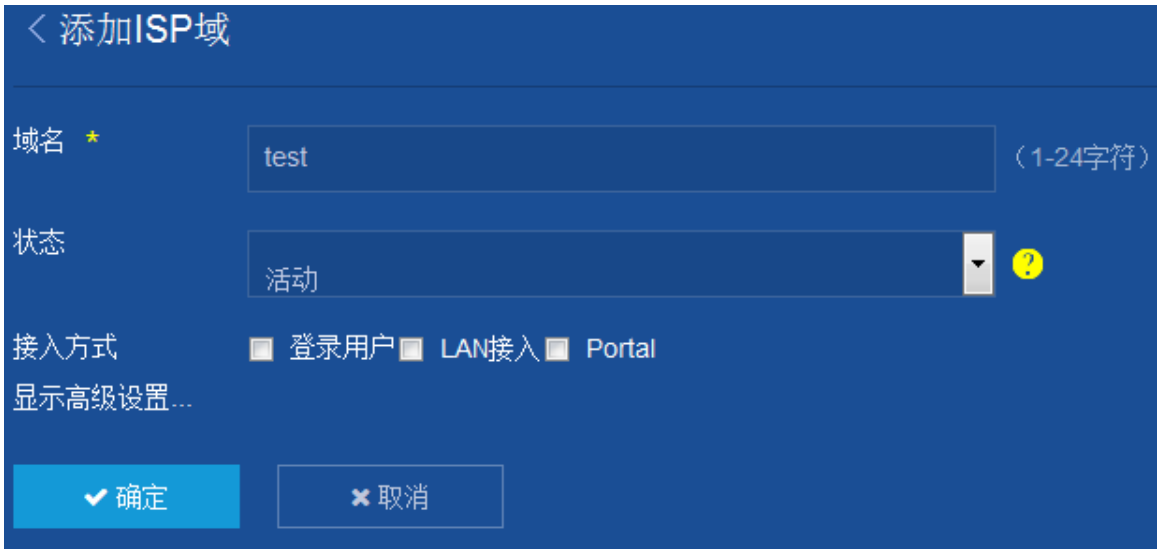
步骤 1：在导航栏中选择“安全 > ISP 域”，进入“ISP 域”页面。

步骤 2：单击。

步骤 3：输入域名为“test”，如下图所示。

步骤 4：单击<确定>按钮完成操作。

图4-12 添加 ISP 域




(3) 添加 ACL 3000。

步骤 1：在导航栏中选择“资源 > IPv4”。

步骤 2：单击，进入新建 ACL 的配置页面。

步骤 3：进行如下配置，如下图所示。

- 选择类型为“高级 ACL”。
- 输入编号为“3000”。

步骤 4：单击<确定>按钮完成操作。

图4-13 添加 ACL 3000


(4) 配置 ACL 规则拒绝目的 IP 地址为 10.0.0.1 的报文通过。

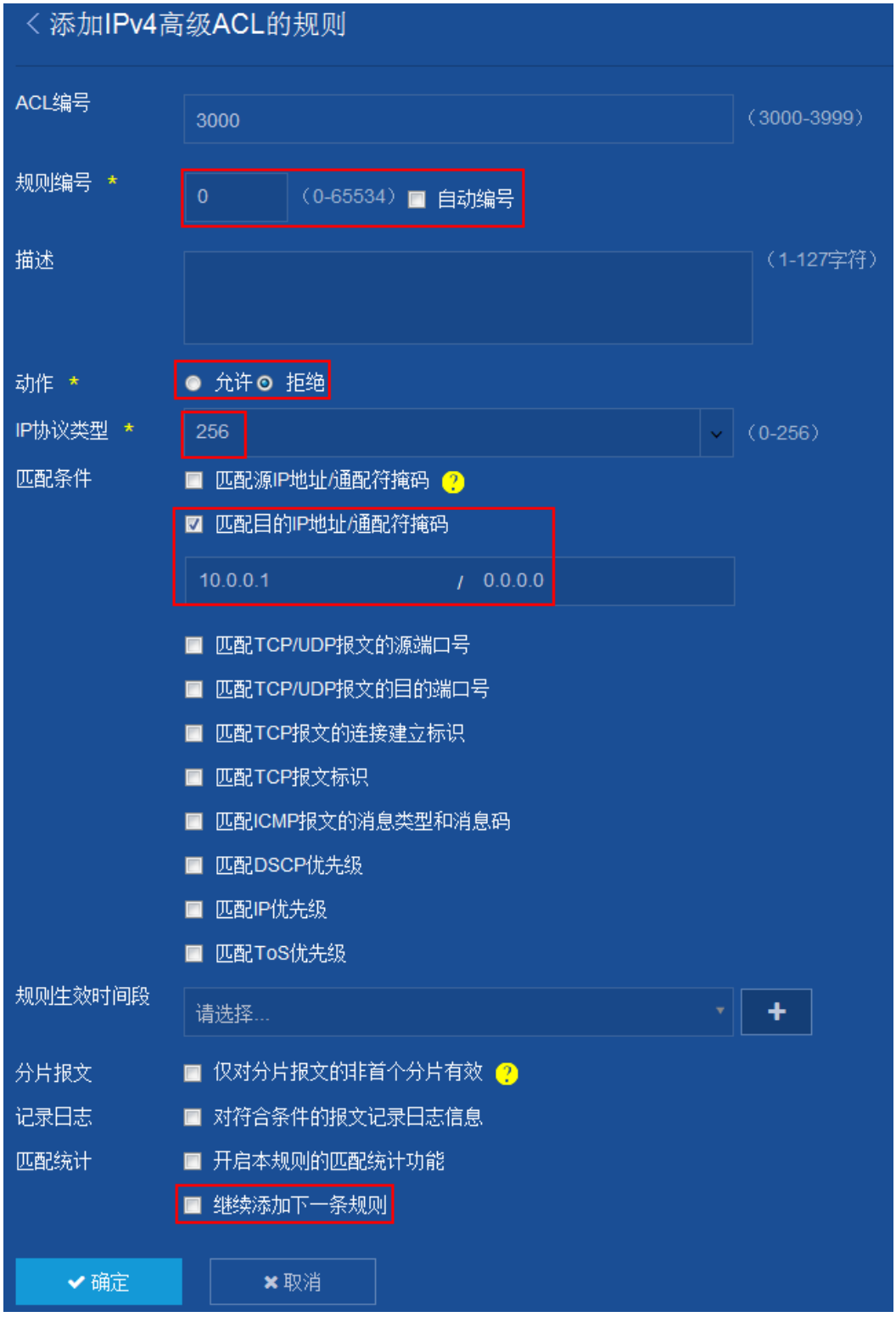
步骤 1：单击“高级配置”页签，进入 ACL 的高级配置页面。

步骤 2：进行如下配置，如下图所示。

- 取消选中“自动编号”前的复选框，输入规则编号为“0”。
- 选择动作为“拒绝”。
- 选择协议类型为 IP，即“256”。
- 选中“匹配目的 IP 地址/通配符掩码”前的复选框，输入目的 IP 地址为“10.0.0.1”。输入目的通配符掩码为“0.0.0.0”。
- 取消选中“继续添加下一条规则”前的复选框。

步骤 3：单击<确定>按钮完成操作。

图4-14 配置 ACL 规则拒绝目的 IP 地址为 10.0.0.1 的报文通过




(5) 配置全局的 MAC 地址认证。

步骤 1：在导航栏中选择“安全 > MAC 地址认证”。

步骤 2：单击“开启 MAC 认证”。

步骤 3：单击  。

步骤 4：在“MAC 地址认证高级设置”中进行如下配置，如下图所示。

- 选择用户名类型为“MAC 地址用户格式”。
- 选择用户认证域为“test”。

步骤 5：单击<确定>按钮完成操作。

图4-15 MAC 地址认证高级设置


(6) 启用端口 GigabitEthernet1/0/1 的 MAC 地址认证。

步骤 1：在导航栏中选择“安全 > MAC 地址认证”，默认进入“MAC 地址认证”页签的页面。

步骤 2：选择端口 GigabitEthernet1/0/1 对应的“开启 MAC 地址认证”下的复选框，如下图所示。

步骤 3：单击<确定>按钮完成操作。

图4-16 启用端口 GigabitEthernet1/0/1 的 MAC 地址认证


### 3. 配置结果验证

用户 Host 认证成功后，通过 ping FTP 服务器，可以验证认证服务器下发的 ACL 3000 是否生效。

```
C:\>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

# 5 端口安全

## 5.1 概述

### 5.1.1 端口安全简介

端口安全是一种基于 MAC 地址对网络接入进行控制的安全机制，是对已有的 802.1X 认证和 MAC 地址认证的扩充。这种机制通过检测端口收到的数据帧中的源 MAC 地址来控制非授权设备对网络的访问，通过检测从端口发出的数据帧中的目的 MAC 地址来控制对非授权设备的访问。

端口安全的主要功能是通过定义各种端口安全模式，让设备学习到合法的源 MAC 地址，以达到相应的网络管理效果。启动了端口安全功能之后，当发现非法报文时，系统将触发相应特性，并按照预先指定的方式进行处理，既方便用户的管理又提高了系统的安全性。这里的非法报文是指：

- 禁止 MAC 地址学习时，收到的源 MAC 地址为未知 MAC 的报文。
- 端口学习到的 MAC 地址达到端口所允许的最大 MAC 地址数后，收到的源 MAC 地址为未知 MAC 的报文。
- 未通过认证的用户发送的报文。

说明

由于端口安全特性通过多种安全模式提供了 802.1X 和 MAC 地址认证的扩展和组合应用，因此在需要灵活使用以上两种认证方式的组网环境下，推荐使用端口安全特性，而在仅需要 802.1X、MAC 地址认证特性来完成接入控制的组网环境下，推荐单独使用以上两个特性，配置过程简洁明了。关于 802.1X、MAC 地址认证特性的详细介绍和具体配置请参见“802.1X”、“MAC 认证”。

### 5.1.2 端口安全的特性

#### 1. 出方向报文控制特性

出方向报文控制特性通过检测从端口发出的数据帧的目的 MAC 地址，保证数据帧只能被发送到已经通过认证的设备上，从而防止非法设备窃听网络数据。该功能暂不支持。

#### 2. 报文入侵控制特性

报文入侵控制特性指通过检测从端口收到的数据帧的源 MAC 地址，对接收非法报文的端口采取相应的安全策略，包括暂时关闭端口、永久关闭端口或阻塞 MAC 地址（默认 3 分钟，不可配），以保证端口的安全性。

#### 3. Trap 特性

Trap 特性是指当端口有特定的数据包（由非法入侵，用户上下线等原因引起）传送时，设备将会发送 Trap 信息，便于网络管理员对这些特殊的行为进行监控。

### 5.1.3 端口安全模式

端口安全包括基本控制和高级控制两种模式：

- 基本控制模式：此模式下，端口通过配置或学习到的安全 MAC 地址被保存在安全 MAC 地址表项中。当端口下的安全 MAC 地址数超过端口允许学习的最大安全 MAC 地址数后，禁止端口学习 MAC 地址，只有源 MAC 地址为安全 MAC 地址、已配置的静态 MAC 地址的报文，才能通过该端口。此模式下，禁止学习动态 MAC 地址。
- 高级控制模式：此模式包括多种安全模式，具体描述如下表所示。

**表5-1 端口安全高级控制模式描述表**

| 高级控制模式类型 | 描述 |
| --- | --- |
| MAC-Auth | 对接入用户采用MAC地址认证<br>此模式下，端口允许多个用户接入 |
| 802.1X Port Based | 对接入用户采用基于端口的802.1X认证<br>此模式下，端口下的第一个802.1X用户认证成功后，其他用户无须认证就可接入<br>需要注意的是，此模式下出方向报文控制特性和报文入侵控制特性不会被触发 |
| 802.1X Single Host | 对接入用户采用基于MAC的802.1X认证<br>此模式下，端口最多只允许一个802.1X认证用户接入 |
| 802.1X MAC Based | 对接入用户采用基于MAC的802.1X认证，<br>此模式下，端口允许多个802.1X认证用户接入 |
| 802.1X MAC Based Or OUI | 与802.1X Single Host模式类似，端口最多只允许一个802.1X认证用户接入<br>• 在用户接入方式为有线的情况下，端口还允许一个指定 OUI 的源 MAC 地址的报文认证通过<br>• 在用户接入方式为无线的情况下，端口首先对报文进行 OUI 检查，OUI 检查失败后再进行 802.1X 认证 |
| MAC-Auth Or 802.1X Single Host | 端口同时处于802.1X Single Host模式和MAC-Auth模式，但802.1X认证优先级大于MAC地址认证<br>• 在用户接入方式为有线的情况下，对于非 802.1X 报文直接进行 MAC 地址认证；对于 802.1X 报文先直接进行 802.1X 认证<br>• 在用户接入方式为无线的情况下，报文首先进行 802.1X 认证，如果 802.1X 认证失败再进行 MAC 地址认证 |
| MAC-Auth Or 802.1X MAC Based | 与MAC-Auth Or 802.1X Single Host类似，但允许端口下有多个802.1X和MAC地址认证用户 |
| MAC-Auth Else 802.1X Single Host | 端口同时处于MAC-Auth模式和802.1X Single Host模式，但MAC地址认证优先级大于802.1X认证<br>对于非802.1X报文直接进行MAC地址认证；对于802.1X报文先进行MAC地址认证，如果MAC地址认证失败进行802.1X认证 |
| MAC-Auth Else 802.1X MAC Based | 与MAC-Auth Else 802.1X Single Host类似，但允许端口下有多个802.1X和MAC地址认证用户 |

说明

- 目前端口安全特性对用户的认证主要有两种方式：MAC 地址认证和 802.1X 认证，不同的安全模式对应不同的认证方式或认证方式组合。
- 当多个用户通过认证时，端口下所允许的最大用户数根据不同的端口安全模式，取最大安全 MAC 地址数与相应模式下允许认证用户数的最小值。例如，802.1X MAC Based 模式下，端口下所允许的最大用户为配置的最大安全 MAC 地址数与 802.1X 认证所允许的最大用户数的最小值。
- OUI（Organizationally Unique Identifier）是 MAC 地址的前 24 位（二进制），是 IEEE（Institute of Electrical and Electronics Engineers，电气和电子工程师学会）为不同设备供应商分配的一个全球唯一的标识符。

# 5.2 配置端口安全

## 5.2.1 配置概述

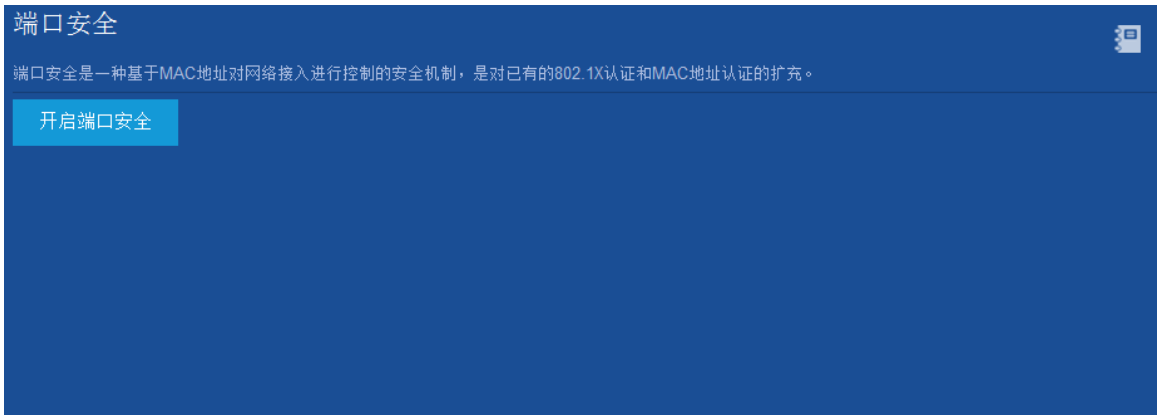
说明

- 在配置端口安全之前，需要关闭全局的 802.1X 和 MAC 地址认证功能。
- 一个端口只能选择配置基本控制模式和高级控制模式中的一种。已进行了基本控制模式配置的端口，不能再配置为高级控制模式；反之亦然。
- 设备暂不支持出方向报文控制特性。

## 5.2.2 配置端口安全

(1) 在导航栏中选择“安全 > 端口安全”，进入“端口安全”页面，如下图所示。

图5-1 开启端口安全




(2) 单击<开启端口安全>按钮，开启端口安全功能，进入如下图所示页面。

说明

单击，可关闭端口安全功能。

图5-2 端口安全


(3) 配置端口安全的信息，详细说明如下表所示。

(4) 单击<确定>按钮完成操作。

表5-2 端口安全

| 标题项 | 说明 |
| --- | --- |
| 端口 | 显示端口号 |
| 端口安全模式 | 设置端口安全模式 |
| 当前用户数 | 显示当前用户数 |
| 高级设置 | 设置高级信息，详细请参见“5.2.3 配置端口高级信息” |

## 5.2.3 配置端口高级信息

(1) 单击<高级设置>按钮，进入如下图所示页面。

图5-3 端口高级设置


(2) 选择认证模式，设置对应参数，以 macAddressElseUserLoginSecureExt 模式为例，如下图所示。

图5-4 认证模式为 macAddressElseUserLoginSecureExt


(3) 单击“端口安全”页签。

(4) 配置端口安全的信息，详细参数请参见下表。

表5-3 端口安全

| 标题项 | 说明 |
| --- | --- |
| 入侵保护模式 | 当设备检测到一个非法的用户通过端口试图访问网络时，入侵检测特性用于配置设备可能对其采取的安全措施，包括以下三种方式：<br>• 阻塞 MAC 地址：表示将非法报文的源 MAC 地址加入阻塞 MAC 地址列表中，源 MAC 地址为阻塞 MAC 地址的报文将被丢弃。此 MAC 地址在被阻塞 3 分钟（系统默认，不可配）后恢复正常<br>• 永久关闭端口：表示将收到非法报文的端口永久关闭<br>• 暂时关闭端口：表示将收到非法报文的端口暂时关闭一段时间 |

| 标题项 | 说明 |
| --- | --- |
| NTK(Need To Know)模式 | Need To Know特性用来限制认证端口上出方向的报文转发，可支持以下三种限制方式：<br>• ntkonly：仅允许目的 MAC 地址为已通过认证的 MAC 地址的单播报文通过<br>• ntk-withbroadcasts：允许目的 MAC 地址为已通过认证的 MAC 地址的单播报文或广播地址的报文通过<br>• ntk-withmulticasts：允许目的 MAC 地址为已通过认证的 MAC 地址的单播报文，广播地址或组播地址的报文通过<br>配置了Need To Know的端口在以上任何一种方式下都不允许目的MAC地址未知的单播报文通过 |
| 安全MAC地址老化模式 | 支持两种老化机制：<br>• 定时老化<br>• 无流量老化。设备会定期检测（检测周期不可配）端口上的安全 MAC 地址是否有流量产生，若某安全 MAC 地址在配置的 Sticky MAC 地址老化时间内没有任何流量产生，则才会被老化 |
| 保存安全MAC地址 | 选择开启或关闭 |
| 忽略授权信息 | 802.1X用户或MAC地址认证用户通过本地认证或RADIUS认证时，本地设备或远程RADIUS服务器会把授权信息下发给用户。通过此配置可实现端口是否忽略这类下发的授权信息 |
| 最大用户数 | 端口安全允许某个端口下有多个用户接入，但是允许的用户数不能超过规定的最大值 |

(5) 单击“802.1X”页签，如下图所示。

图5-5 802.1X


(6) 根据需要配置参数，详细参数说明请参见下表。

表5-4 802.1X

| 标题项 | 说明 |
| --- | --- |
| 周期性重认证 | 端口启动了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定期向该端口在线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） |
| 在线用户握手 | 开启设备的在线用户握手功能后，设备会定期向通过802.1X认证的在线用户发送握手 |

| 标题项 | 说明 |
| --- | --- |
| 安全握手 | 报文，以定期检测用户的在线情况。如果设备连续多次没有收到客户端的响应报文，则会将用户置为下线状态<br>在线用户握手功能处于开启状态的前提下，还可以通过开启在线用户握手安全功能，来防止在线的802.1X认证用户使用非法的客户端与设备进行握手报文的交互，而逃过代理检测、双网卡检测等iNode客户端的安全检查功能。开启了在线用户握手安全功能的设备通过检验客户端上传的握手报文中携带的验证信息，来确认用户是否使用iNode客户端进行握手报文的交互。如果握手检验不通过，则会将用户置为下线状态<br>需要注意的是：在线用户握手安全功能的实现依赖于在线用户握手功能。为使在线用户握手安全功能生效，请保证在线用户握手功能处于开启状态 |
| 单播触发<br>组播触发 | 端口上开启认证触发功能后，设备会主动向该端口上的客户端发送认证请求来触发认证，以支持不能主动发送EAPOL-Start报文来发起认证的客户端。设备提供了以下两种类型的认证触发功能：<br>• 组播触发功能：启用了该功能的端口会定期向客户端组播发送 EAP-Request/Identity 报文来检测客户端并触发认证。该功能用于支持不能主动发起认证的客户端<br>• 单播触发功能：当启用了该功能的端口收到源 MAC 地址未知的报文时，会主动向该 MAC 地址单播发送 EAP-Request/Identity 报文，若端口在指定的时间内没有收到客户端的响应，则重发该报文。该功能适用于客户端不支持主动认证，且仅部分客户端需要进行认证的组网环境，可避免不希望认证或已认证的客户端收到多余的认证触发报文<br>提示<br>建议组播触发功能和单播触发功能不要同时开启，以免认证报文重复发送。 |
| Smarton | 选择开启或关闭 |
| Auth-Fail VLAN | Auth-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Auth-Fail VLAN。需要注意的是，这里的认证失败是认证服务器因某种原因明确拒绝用户认证通过，比如用户密码错误，而不是认证超时或网络连接等原因造成的认证失败 |
| Guest VLAN | 根据需要选择VLAN Guest VLAN功能允许用户在未认证的情况下，访问某一特定VLAN中的资源。这个特定的VLAN称之为Guest VLAN，该VLAN内通常放置一些用于用户下载客户端软件或其他升级程序的服务器<br>根据端口的接入控制方式不同，Guest VLAN的生效情况有所不同 |
| Critical VLAN | 802.1X认证的Critical VLAN功能允许用户在进行802.1X认证时，当所有认证服务器都不可达的情况下访问某一特定VLAN中的资源，这个VLAN称之为802.1X认证的Critical VLAN |
| 端口的强制认证ISP域 | 设置端口的强制认证ISP域 |
| 重认证不可达动作 | 包括下线或上线 |

(7) 单击“MAC 地址认证”页签，如下图所示。

图5-6 MAC 地址认证


(8) 根据需要配置参数，详细参数说明请参见下表。

表5-5 MAC 地址认证

| 标题项 | 说明 |
| --- | --- |
| 延迟认证 | 在端口上同时启用了802.1X认证和MAC地址认证功能的情况下，可以通过启用MAC地址认证延时触发功能达到优先触发802.1X认证的目的。具体是否需要启用此功能，可以根据实际组网情况进行相应设置。 |
| 多VLAN功能 | 包括单 VALN 模式和多 VALN 模式 |
| Guest VLAN | Guest 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，比如获取客户端软件，升级客户端或执行其他一些用户升级程序。这个VLAN称之为Guest VLAN。 |
| Critical VLAN | MAC地址认证的Critical VLAN功能允许用户在进行MAC地址认证时，当所有认证服务器都不可达的情况下访问某一特定VLAN中的资源，这个VLAN称之为MAC地址认证的Critical VLAN。 |
| 重认证服务器不可达用户在线状态 | 包括强制用户下线和保持用户上线 |

(9) 单击<确定>按钮完成操作。

### 5.2.4 配置端口安全高级信息

(1) 单击  可进行端口安全高级设置，如下图所示。

图5-7 端口安全高级设置


(2) 根据需要设置参数，详细参数说明请参见下表。

表5-6 端口安全高级设置参数说明

| 标题项 | 说明 |
| --- | --- |
| 授权失败用户下线 | 显示授权失败用户的 ON/OFF 状态 |
| 安全MAC地址老化时长 | 设置安全 MAC 地址的老化时长 |
| 端口暂时关闭时长 | 设置端口暂时关闭的时长 |
| 802.1X高级设置 | 详细参数说明如表5-4所示 |
| MAC地址认证高级设置 | 详细参数说明如表5-5所示 |
| 认证OUIMAC | 设置索引和OUIMAC |

# 6 Portal

## 6.1 Portal简介

### 6.1.1 Portal 概述

Portal 在英语中是入口的意思。Portal 认证通常也称为 Web 认证，即通过 Web 页面接受用户输入的用户名和密码，对用户进行身份认证，以达到对用户访问进行控制的目的。在采用了 Portal 认证的组网环境中，未认证用户上网时，接入设备强制用户登录到特定站点，用户可以免费访问其中的服务；当用户需要使用互联网中的其它信息时，必须在 Portal Web 服务器提供的网站上进行 Portal 认证，只有认证通过后才可以使用这些互联网中的设备或资源。

根据是否为用户主动发起认证，可以将 Portal 认证分为主动认证和强制认证两种类型：用户可以主动访问已知的 Portal Web 服务器网站，输入用户名和密码进行认证，这种开始 Portal 认证的方式称作主动认证；用户访问任意非 Portal Web 服务器网站时，被强制访问 Portal Web 服务器网站，继而开始 Portal 认证的过程称作强制认证。

Portal 认证是一种灵活的访问控制技术，可以在接入层以及需要保护的关键数据入口处实施访问控制，具有如下优势：

- 可以不安装客户端软件，直接使用 Web 页面认证，使用方便。
- 可以为运营商提供方便的管理功能和业务拓展功能，例如运营商可以在认证页面上开展广告、社区服务、信息发布等个性化的业务。
- 支持多种组网型态，例如二次地址分配认证方式可以实现灵活的地址分配策略且能节省公网 IP 地址，可跨三层认证方式可以跨网段对用户作认证。

目前，设备支持的 Portal 版本为 Portal 1.0、Portal 2.0 和 Portal 3.0。

### 6.1.2 Portal 安全扩展功能

Portal 的安全扩展功能是指，在 Portal 身份认证的基础之上，通过强制接入终端实施补丁和防病毒策略，加强网络终端对病毒攻击的主动防御能力。具体的安全扩展功能如下：

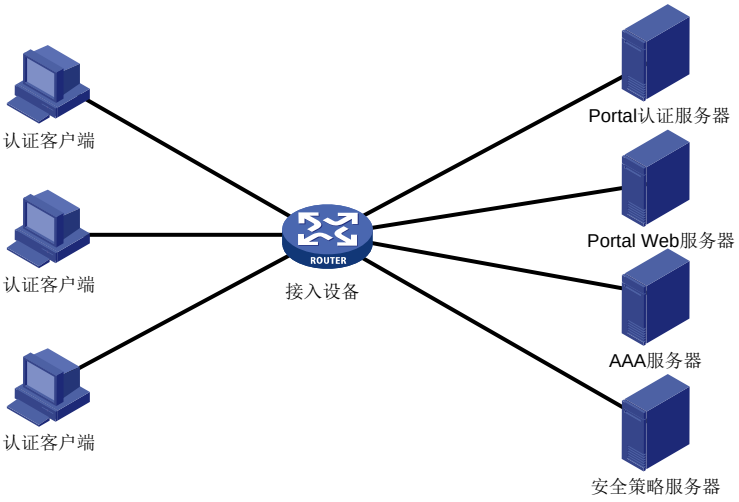
- 安全性检测：在对用户的身份认证的基础上增加了安全认证机制，可以检测接入终端上是否安装了防病毒软件、是否更新了病毒库、是否安装了非法软件、是否更新了操作系统补丁等；
- 访问资源受限：用户通过身份认证后仅仅获得访问指定互联网资源的权限，如病毒服务器、操作系统补丁更新服务器等；当用户通过安全认证后便可以访问更多的互联网资源。

安全性检测功能必须与 iMC 安全策略服务器以及 iNode 客户端配合使用。

### 6.1.3 Portal 的系统组成

Portal 的典型组网方式如图 6-1 所示，它由六个基本要素组成：认证客户端、接入设备、Portal 认证服务器、Portal Web 服务器、AAA 服务器和安全策略服务器。

图6-1 Portal 系统组成示意图




### 2. 认证客户端

用户终端的客户端系统，为运行 HTTP/HTTPS 协议的浏览器或运行 Portal 客户端软件的主机。对用户终端的安全性检测是通过 Portal 客户端和安全策略服务器之间的信息交流完成的。

### 3. 接入设备

交换机、路由器等宽带接入设备的统称，主要有三方面的作用：

- 在认证之前，将用户的所有 HTTP 请求都重定向到 Portal Web 服务器。
- 在认证过程中，与 Portal 认证服务器、AAA 服务器交互，完成身份认证/授权/计费的功能。
- 在认证通过后，允许用户访问被授权的互联网资源。

### 4. Portal 认证服务器

接收 Portal 客户端认证请求的服务器端系统，与接入设备交互认证客户端的认证信息。

### 5. Portal Web 服务器

负责向客户端提供 Web 认证页面，并将客户端的认证信息（用户名、密码等）提交给 Portal 认证服务器。Portal Web 服务器通常与 Portal 认证服务器是一体的，也可以是独立的服务器端系统。

### 6. AAA 服务器

与接入设备进行交互，完成对用户的认证、授权和计费。目前仅 RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）服务器支持对 Portal 用户进行认证、授权和计费。

### 7. 安全策略服务器

与 Portal 客户端、接入设备进行交互，完成对用户的安全检测，并对用户进行安全授权操作。

## 6.1.4 使用本地 Portal Web 服务器的 Portal 系统

### 1. 系统组成

本地 Portal Web 服务器功能是指，Portal 认证系统中不采用外部独立的 Portal Web 服务器和 Portal 认证服务器，而由接入设备实现 Portal Web 服务器和 Portal 认证服务器功能。这种情况下，Portal 认证系统仅包括三个基本要素：认证客户端、接入设备和 AAA 服务器，如图 6-2 所示。由于设备支

持 Portal 用户进行本地 Portal 认证，因此就不需要部署额外的 Portal Web 和 Portal 认证服务器，增强了 Portal 认证的通用性。

图6-2 使用本地 Portal Web 服务器的 Portal 系统组成示意图


说明

- 使用本地 Portal Web 服务器的 Portal 认证系统不支持 Portal 扩展功能，因此使用本地 Portal Web 服务器的网络环境中不需要部署安全策略服务器。
- 内嵌本地 Portal Web 服务器的接入设备实现了简单的 Portal Web 服务器和 Portal 认证服务器功能，仅能给用户提供通过 Web 方式登录、下线的基本功能，并不能完全替代独立的 Portal 服务器。
- 不支使用 iNode 客户端方式的 Portal 认证。

### 2. 认证客户端和本地 Portal Web 服务器之间的交互协议

认证客户端和内嵌本地 Portal Web 服务器的接入设备之间可以采用 HTTP 和 HTTPS 协议通信。若客户端和接入设备之间交互 HTTP 协议，则报文以明文形式传输，安全性无法保证；若客户端和接入设备之间交互 HTTPS 协议，则报文基于 SSL 提供的安全机制以密文的形式传输，数据的安全性有保障。

### 3. 本地 Portal Web 服务器支持用户自定义认证页面

本地 Portal Web 服务器支持由用户自定义认证页面的内容，即允许用户编辑一套或多套认证页面的 HTML 文件，并将其压缩之后保存至设备的存储介质的根目录中。每套自定义页面文件中包括六个认证页面：登录页面、登录成功页面、在线页面、下线成功页面、登录失败页面和系统忙碌页面。本地 Portal Web 服务器根据不同的认证阶段向客户端推出对应的认证页面。

## 6.1.5 Portal 的基本交互过程

Portal 系统中各基本要素的交互过程如下：

(1) 未认证用户访问网络时，在 Web 浏览器地址栏中输入一个互联网的地址，那么此 HTTP 请求在经过接入设备时会被重定向到 Portal Web 服务器的 Web 认证主页上。用户也可以主动登录 Portal Web 服务器的 Web 认证主页。若需要使用 Portal 的安全扩展认证功能，则用户必须使用 iNode 客户端。

(2) 用户在认证主页/认证对话框中输入认证信息后提交，Portal Web 服务器会将用户的认证信息传递给 Portal 认证服务器，由 Portal 认证服务器处理并转发给接入设备。

(3) 接入设备与 AAA 服务器交互进行用户的认证、授权和计费。

(4) 认证通过后，如果未对用户采用安全策略，则接入设备会打开用户与互联网的通路，允许用户访问互联网；如果对用户采用了安全策略，则客户端、接入设备与安全策略服务器交互，对用户的安全检测通过之后，安全策略服务器根据用户的安全性授权用户访问非受限资源。目前通

过访问 Web 页面进行的 Portal 认证不能对用户实施安全策略检查，安全检查功能的实现需要与 iNode 客户端配合。

说明

无论是 Web 客户端还是 iNode 客户端发起的 Portal 认证，均能支持 Portal 认证穿越 NAT，即 Portal 客户端位于私网、Portal 认证服务器位于公网。

### 6.1.6 Portal 的认证方式

Portal 支持三种认证方式：直接认证方式、二次地址分配认证方式和可跨三层认证方式。直接认证方式和二次地址分配认证方式下，认证客户端和接入设备之间没有三层转发设备；可跨三层认证方式下，认证客户端和接入设备之间可以（但不必须）跨接三层转发设备。

#### 1. 直接认证方式

用户在认证前通过手工配置或 DHCP 直接获取一个 IP 地址，只能访问 Portal Web 服务器，以及设定的免认证地址；认证通过后即可访问网络资源。认证流程相对简单。

#### 2. 二次地址分配认证方式

用户在认证前通过 DHCP 获取一个私网 IP 地址，只能访问 Portal Web 服务器，以及设定的免认证地址；认证通过后，用户会申请到一个公网 IP 地址，即可访问网络资源。该认证方式解决了 IP 地址规划和分配问题，对未认证通过的用户不分配公网 IP 地址。例如运营商对于小区宽带用户只在访问小区外部资源时才分配公网 IP。目前，仅 iNode 客户端支持该认证方式。需要注意的是，IPv6 Portal 认证不支持二次地址分配方式。

#### 3. 可跨三层认证方式

和直接认证方式基本相同，但是这种认证方式允许认证用户和接入设备之间跨越三层转发设备。

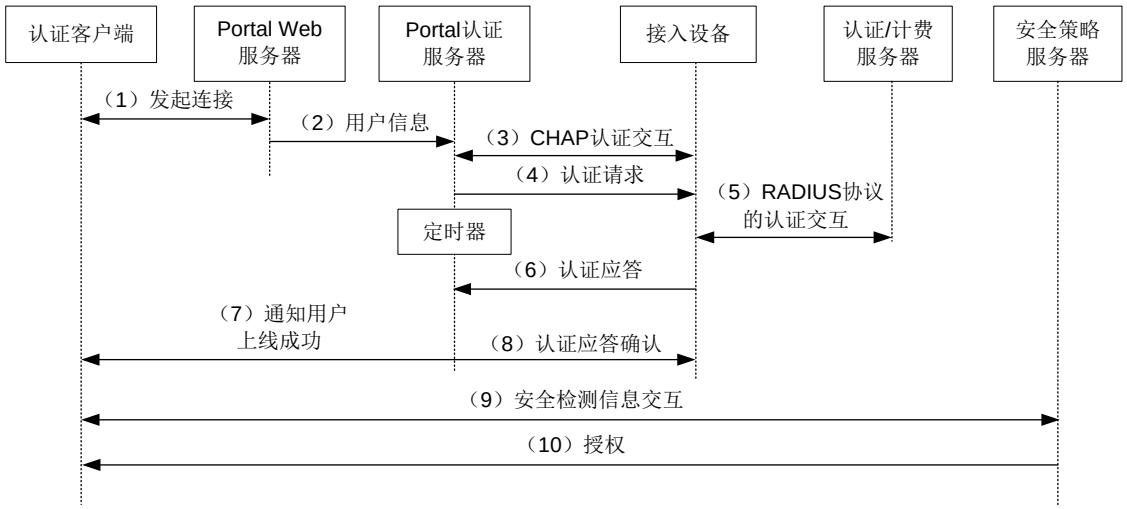
对于以上三种认证方式，IP 地址都是用户的唯一标识。接入设备基于用户的 IP 地址下发 ACL 对接口上通过认证的用户报文转发进行控制。由于直接认证和二次地址分配认证下的接入设备与用户之间未跨越三层转发设备，因此接口可以学习到用户的 MAC 地址，接入设备可以利用学习到 MAC 地址增强对用户报文转发的控制力度。

### 6.1.7 Portal 认证流程

直接认证和可跨三层 Portal 认证流程相同。二次地址分配认证流程因为有两次地址分配过程，所以其认证流程和另外两种认证方式有所不同。

### 1. 直接认证和可跨三层 Portal 认证的流程（CHAP/PAP 认证方式）

图6-3 直接认证/可跨三层 Portal 认证流程图




直接认证/可跨三层 Portal 认证流程：

(2) Portal 用户通过 HTTP 协议访问外部网络。HTTP 报文经过接入设备时，对于访问 Portal Web 服务器或设定的免认证地址的 HTTP 报文，接入设备允许其通过；对于访问其它地址的 HTTP 报文，接入设备将其重定向到 Portal Web 服务器。Portal Web 服务器提供 Web 页面供用户输入用户名和密码。

(3) Portal Web 服务器将用户输入的信息提交给 Portal 认证服务器进行认证。

(4) Portal 认证服务器与接入设备之间进行 CHAP（Challenge Handshake Authentication Protocol，质询握手验证协议）认证交互。若采用 PAP（Password Authentication Protocol，密码验证协议）认证则直接进入下一步骤。采用哪种认证交互方式由 Portal 认证服务器决定。

(5) Portal 认证服务器将用户输入的用户名和密码组装成认证请求报文发往接入设备，同时开启定时器等待认证应答报文。

(6) 接入设备与 RADIUS 服务器之间进行 RADIUS 协议报文的交互。

(7) 接入设备向 Portal 认证服务器发送认证应答报文，表示认证成功或者认证失败。

(8) Portal 认证服务器向客户端发送认证成功或认证失败报文，通知客户端认证成功（上线）或失败。

(9) 若认证成功，Portal 认证服务器还会向接入设备发送认证应答确认。若是 iNode 客户端，则还需要进行以下安全扩展功能的步骤，否则 Portal 认证过程结束，用户上线。

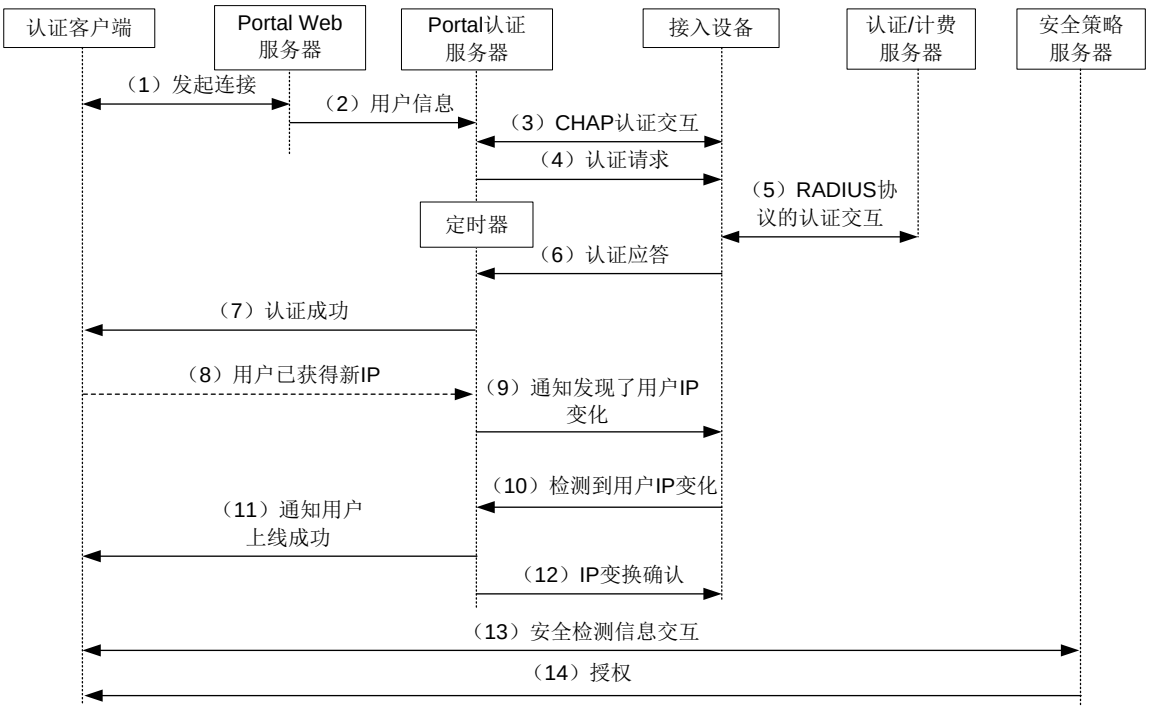
(10) 客户端和安全策略服务器之间进行安全信息交互。安全策略服务器检测客户端的安全性是否合格，包括是否安装防病毒软件、是否更新病毒库、是否安装了非法软件、是否更新操作系统补丁等。

(11) 安全策略服务器根据安全检查结果授权用户访问指定的网络资源，授权信息保存到接入设备中，接入设备将使用该信息控制用户的访问。

步骤(9)、(10)为 Portal 认证安全扩展功能的交互过程。

## 2. 二次地址分配认证方式的流程（CHAP/PAP 认证方式）

图6-4 二次地址分配认证方式流程图




二次地址分配认证流程：

(1)～(7)同直接/可跨三层 Portal 认证中步骤（1）～（7）。

(8) 客户端收到认证通过报文后，通过 DHCP 获得新的公网 IP 地址，并通知 Portal 认证服务器用户已获得新 IP 地址。

(9) Portal 认证服务器通知接入设备客户端获得新公网 IP 地址。

(10) 接入设备通过 DHCP 模块得知用户 IP 地址变化后，通告 Portal 认证服务器已检测到用户 IP 变化。

(11) 当 Portal 认证服务器接收到客户端以及接入设备发送的关于用户 IP 变化的通告后，通知客户端上线成功。

(12) Portal 认证服务器向接入设备发送 IP 变化确认报文。

(13) 客户端和安全策略服务器之间进行安全信息交互。安全策略服务器检测客户端的安全性是否合格，包括是否安装防病毒软件、是否更新病毒库、是否安装了非法软件、是否更新操作系统补丁等。

(14) 安全策略服务器根据用户的安全性授权用户访问指定的网络资源，授权信息保存到接入设备中，接入设备将使用该信息控制用户的访问。

步骤(13)、(14)为 Portal 认证扩展功能的交互过程。

## 6.2 配置准备

Portal 提供了一个用户身份认证和安全认证的实现方案，但是仅仅依靠 Portal 不足以实现该方案。接入设备的管理者需选择使用 RADIUS 认证方法，以配合 Portal 完成用户的身份认证。Portal 认证的配置前提：

- Portal 认证服务器、Portal Web 服务器、RADIUS 服务器已安装并配置成功。
- 若采用二次地址分配认证方式，接入设备需启动 DHCP 中继功能，另外需要安装并配置好 DHCP 服务器。
- 用户、接入设备和各服务器之间路由可达。
- 如果通过远端 RADIUS 服务器进行认证，则需要在 RADIUS 服务器上配置相应的用户名和密码，然后在接入设备端进行 RADIUS 客户端的相关设置。
- 如果需要支持 Portal 的安全扩展功能，需要安装并配置 CAMS EAD/iMC EAD 安全策略组件。同时保证在接入设备上的 ACL 配置和安全策略服务器上配置的隔离 ACL 的编号、安全 ACL 的编号对应。

## 6.3 配置Portal

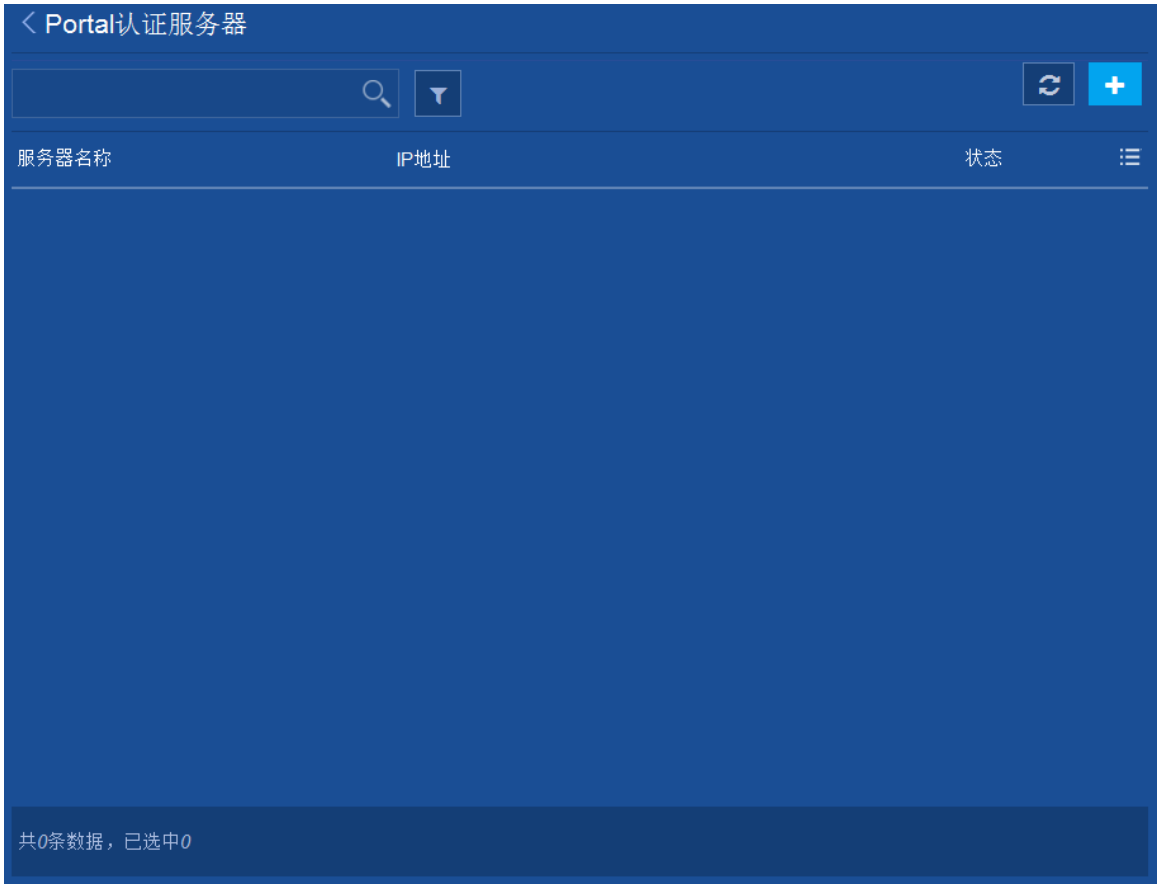
在导航栏中选择“安全 > Portal”，进入“Portal”页面，如下图所示。

图6-5 Portal


### 6.3.1 配置 Portal 认证服务器

(1) 单击“Portal 认证服务器”后的，进入“Portal 认证服务器”页面，如下图所示。

图6-6 Portal 认证服务器




(2) 单击  可创建 Portal 认证服务器，进入“创建 Portal 认证服务器”页面，如下图所示。

图6-7 创建 Portal 认证服务器


(3) 根据需要设置参数，详细参数说明如下表所示。

(4) 单击<确定>按钮完成操作。

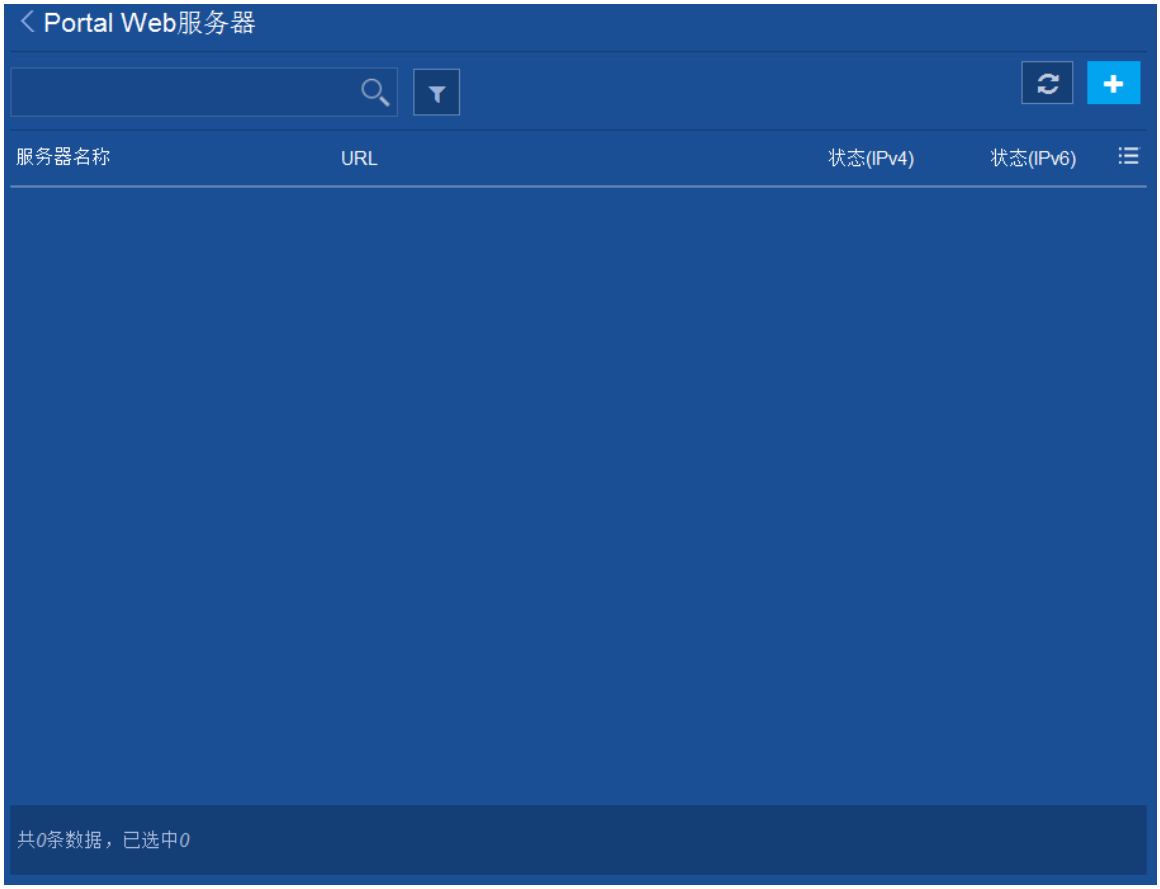
表6-1 创建 Portal 认证服务器的参数说明

| 标题项 | 说明 |
| --- | --- |
| 服务器名称 | 设置服务器名称 |
| IP地址 | 设置 Portal 认证服务器的 IP 地址 |
| 共享密钥 | 设置共享密钥 |
| 服务器监听端口号 | 设置服务器监听端口号 |
| 服务器可达性探测 | 选择开启或关闭。 |
| 用户信息同步 | 选择开启或关闭。 |

## 6.3.2 配置 Portal Web 服务器

(1) 单击“Portal Web 服务器”后的，进入“Portal Web 服务器”页面，如下图所示。

图6-8 Portal Web 服务器




(2) 单击可创建 Portal Web 服务器，进入“创建 Portal Web 服务器”页面，如下图所示。

图6-9 创建 Portal Web 服务器


(3) 根据需要设置参数，详细参数说明如下表所示。

(4) 单击<确定>按钮完成操作。

表6-2 创建 Portal Web 服务器的参数说明

| 标题项 | | 说明 |
|---|---|---|
| 服务器名称 | | 设置服务器名称 |
| URL | | 设置 Portal Web 服务器 URL |
| URL携带的参数 | URL参数名 | 输入URL的参数名 |
| | 用户的IP地址 | 单击“用户的IP地址”前的单选框，表示选中该参数 |
| | 用户的MAC地址 | 单击“用户的MAC地址”前的单选框，表示选中该参数 |
| | 初始访问的URL | 单击“初始访问的URL”前的单选框，表示选中该参数 |
| | 自定义URL参数 | 单击“自定义URL参数”前的单选框，表示选中该参数 |
| 服务器可达性探测 | | 选择开启或关闭 |

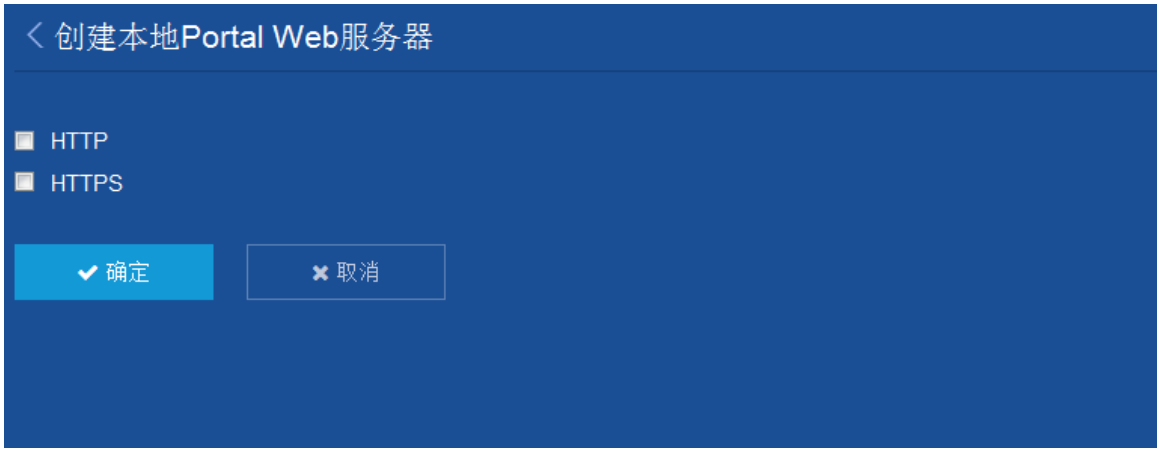
### 6.3.3 配置本地 Portal Web 服务器

(1) 单击“本地 Portal Web 服务器”后的，进入“本地 Portal Web 服务器”页面，如下图所示。

图6-10 本地 Portal Web 服务器


(2) 单击可创建本地 Portal Web 服务器，进入“创建本地 Portal Web 服务器”页面，如下图所示。

图6-11 创建本地 Portal Web 服务器




(3) 根据需要设置参数，详细参数说明如下表所示。

(4) 单击<确定>按钮完成操作。

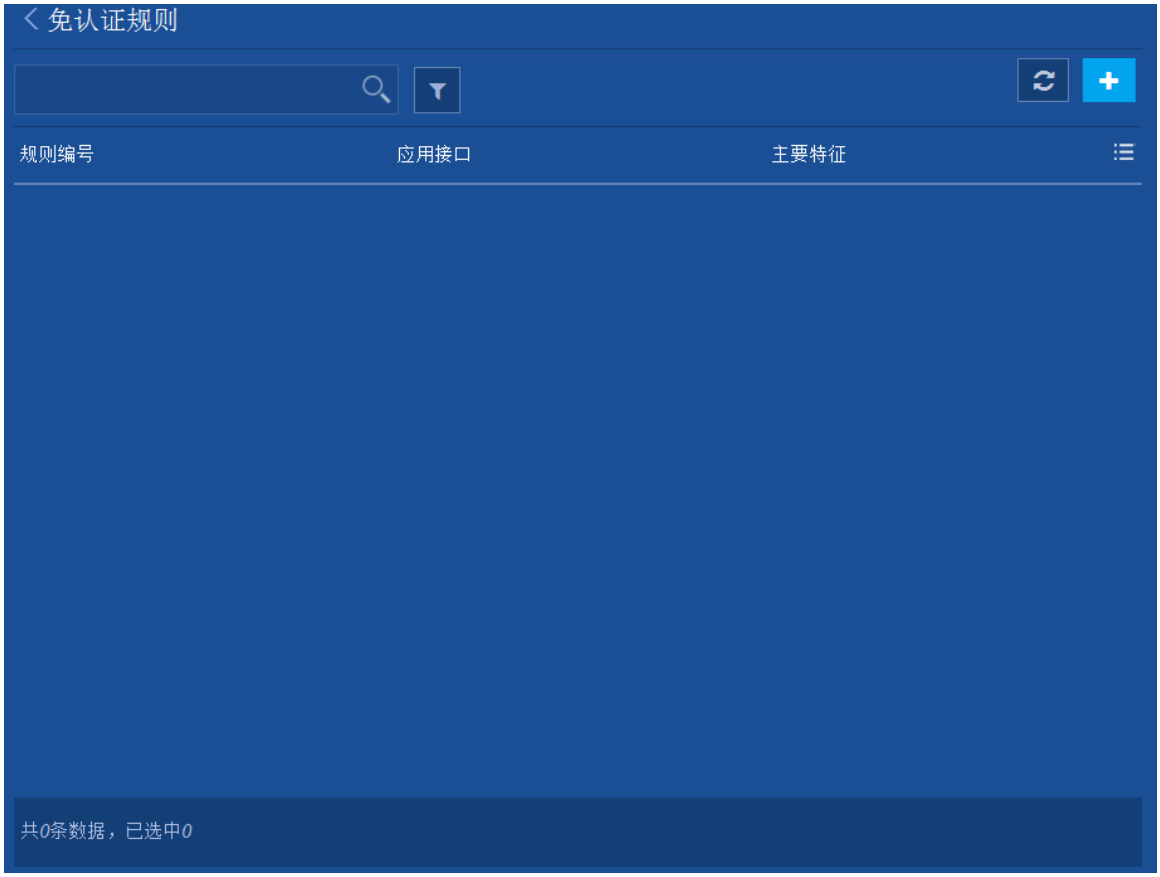
表6-3 创建本地 Portal Web 服务器的参数说明

| 标题项 | 说明 |
| --- | --- |
| HTTP | 认证客户端和内嵌本地Portal Web 服务器的接入设备之间可以采用HTTP和HTTPS协议通信<br>• 若客户端和接入设备之间交互 HTTP 协议，则报文以明文形式传输，安全性无法保证<br>• 若客户端和接入设备之间交互 HTTPS 协议，则报文基于 SSL 提供的安全机制以密文的形式传输，数据的安全性有保障 |
| HTTPS | |

## 6.3.4 配置免认证规则

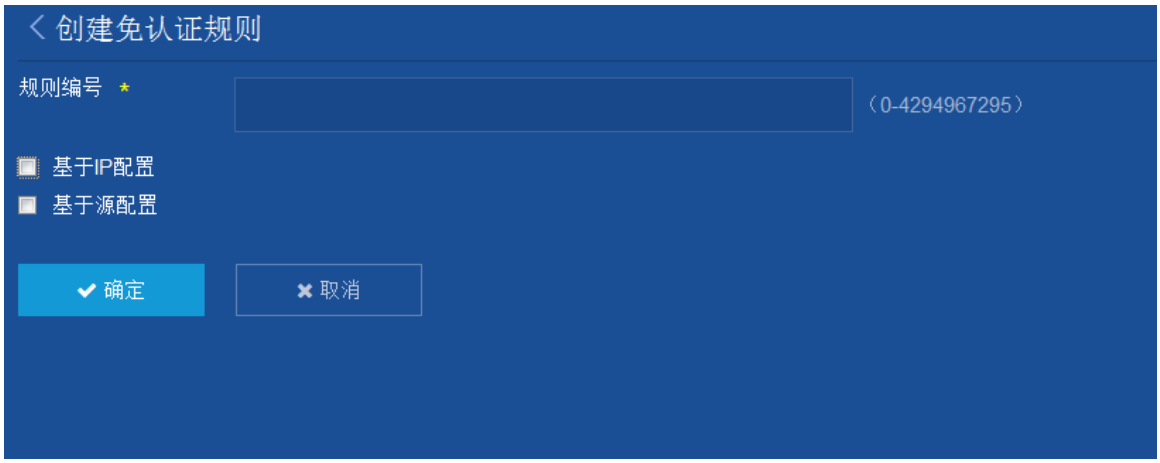
(1) 单击“免认证规则”后的，进入“免认证规则”页面，如下图所示。

图6-12 免认证规则




(2) 单击  可创建免认证规则，进入“创建免认证规则”页面，如下图所示。

图6-13 创建免认证规则




(3) 根据需要设置参数，详细参数说明如下表所示。

(4) 单击<确定>按钮完成操作。

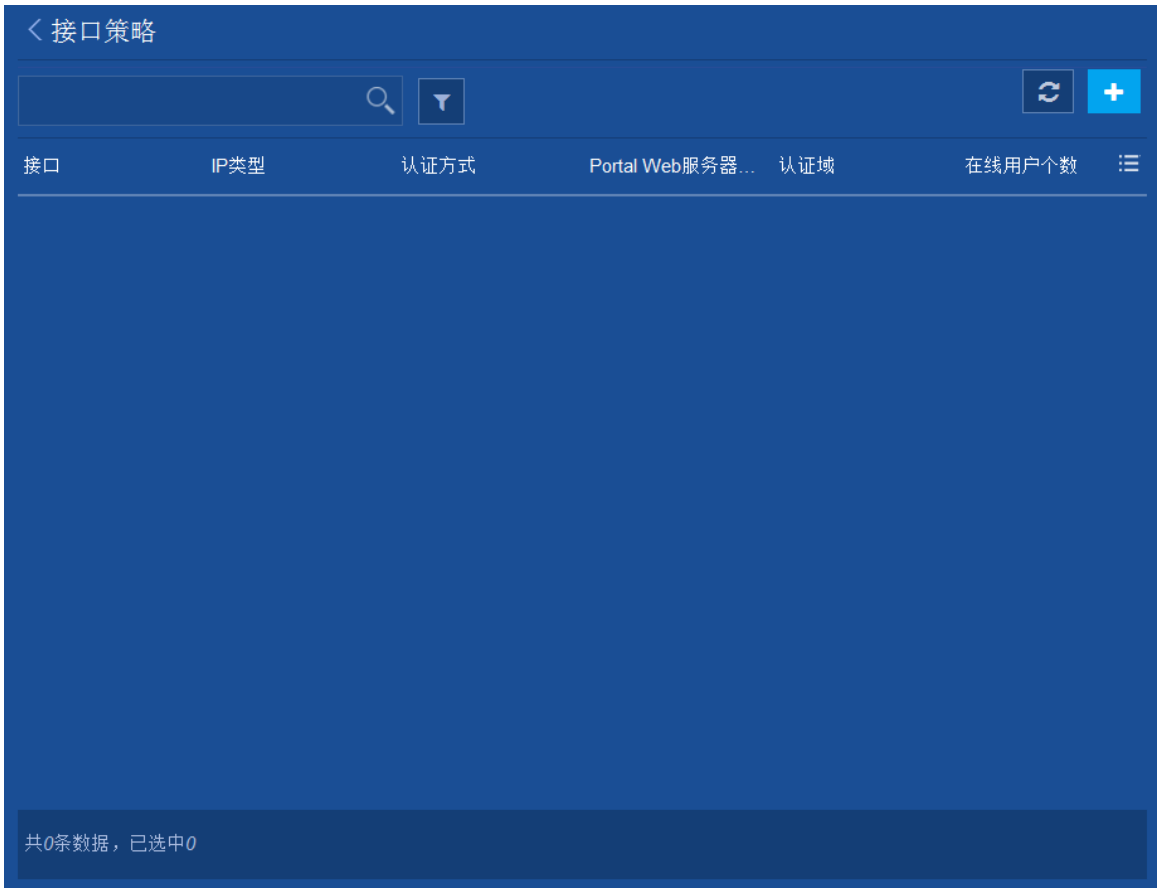
表6-4 创建免认证规则的参数说明

| 标题项 | 说明 |
| --- | --- |
| 规则编号 | 设置规则编号 |
| 基于IP配置 | 根据需要选择复选框，并进行相关设置 |
| 基于源配置 | 根据需要选择复选框，并进行相关设置 |

## 6.3.5 配置接口策略

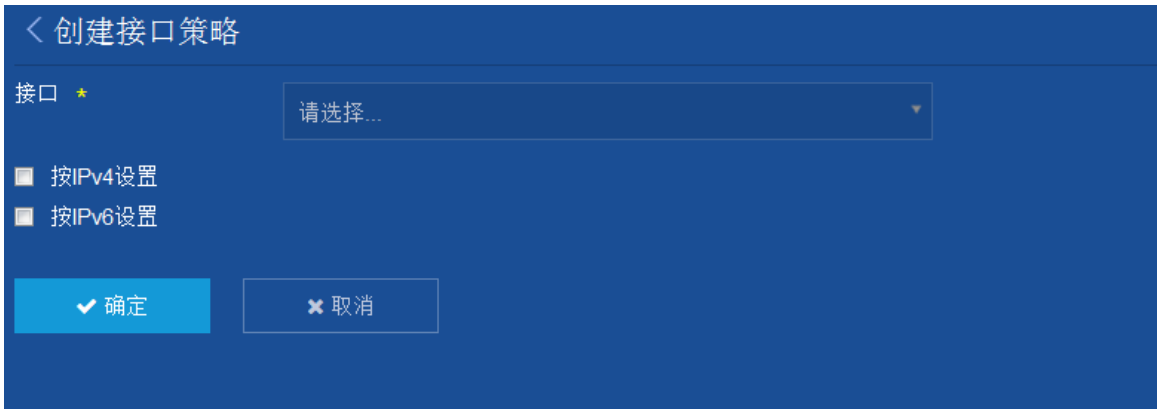
(1) 单击“接口策略”后的，进入“接口策略”页面，如下图所示。

图6-14 接口策略




(2) 单击可创建接口策略，进入“创建接口策略”页面，如下图所示。

图6-15 创建接口策略




(3) 根据需要设置参数，详细参数说明如所示。

(4) 单击<确定>按钮完成操作。

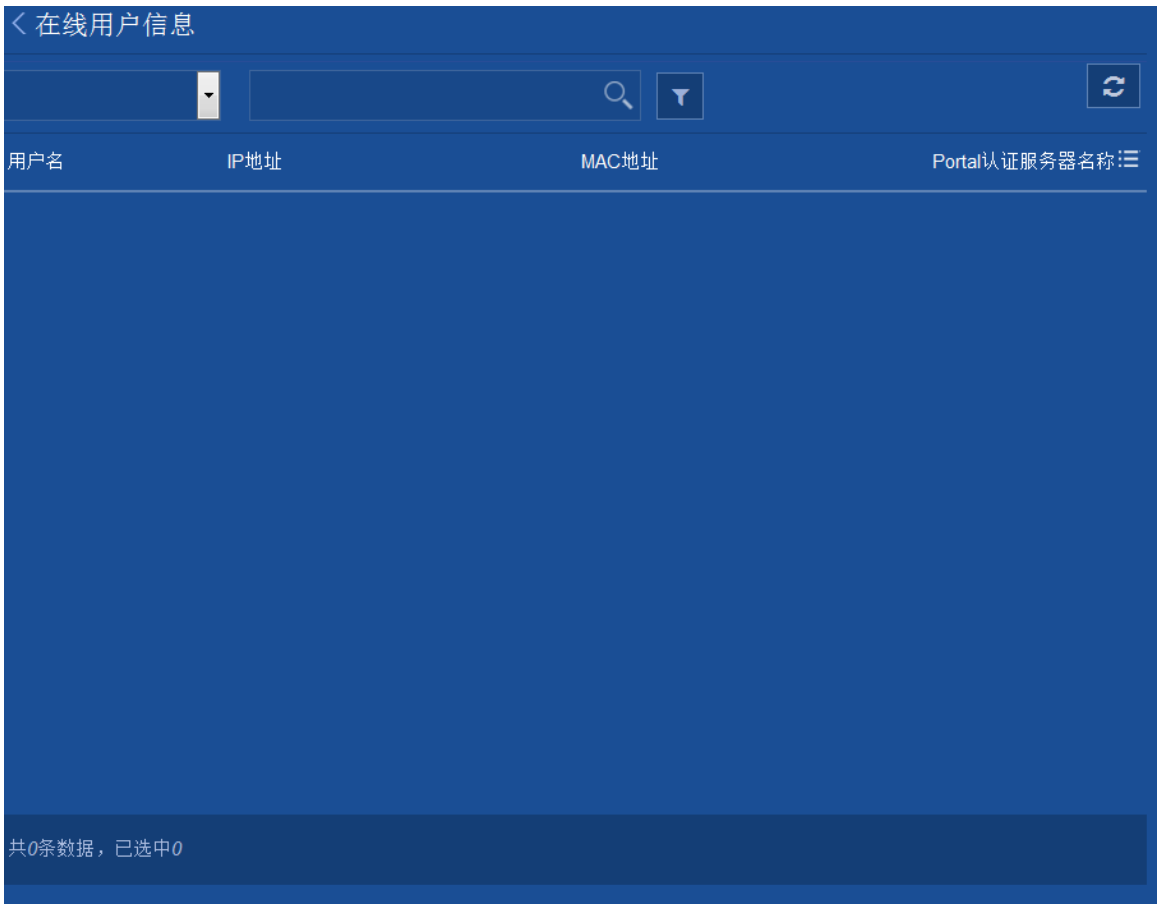
表6-5 创建接口策略

| 标题项 | 说明 |
| --- | --- |
| 接口 | 选择接口 |
| 按IPv4设置 | 根据需要选择复选框，并进行相关设置 |
| 按IPv6设置 | 根据需要选择复选框，并进行相关设置 |

### 6.3.6 查看在线用户信息

单击“在线用户信息”后的，进入“在线用户信息”页面，如下图所示。可查看在线用户的 IP 地址和 MAC 地址等信息。

图6-16 在线用户信息



# 7 ISP 域

## 7.1 ISP域简介

一个 ISP（Internet Service Provider，互联网服务提供商）域是由属于同一个 ISP 的用户构成的群体。

在“*userid@isp-name*”形式的用户名中，“*userid*”为用于身份认证的用户名，“*isp-name*”为域名。

在多 ISP 的应用环境中，不同 ISP 域的用户有可能接入同一台设备。而且各 ISP 用户的用户属性（例如用户名及密码构成、服务类型/权限等）有可能不相同，因此有必要通过设置 ISP 域把它们区分开，并为每个 ISP 域单独配置包括 AAA 策略（一组不同的认证/授权/计费方案）在内的属性集。

对于设备来说，每个接入用户都属于一个 ISP 域。如果某个用户在登录时没有提供 ISP 域名，系统将把它归于缺省的 ISP 域。

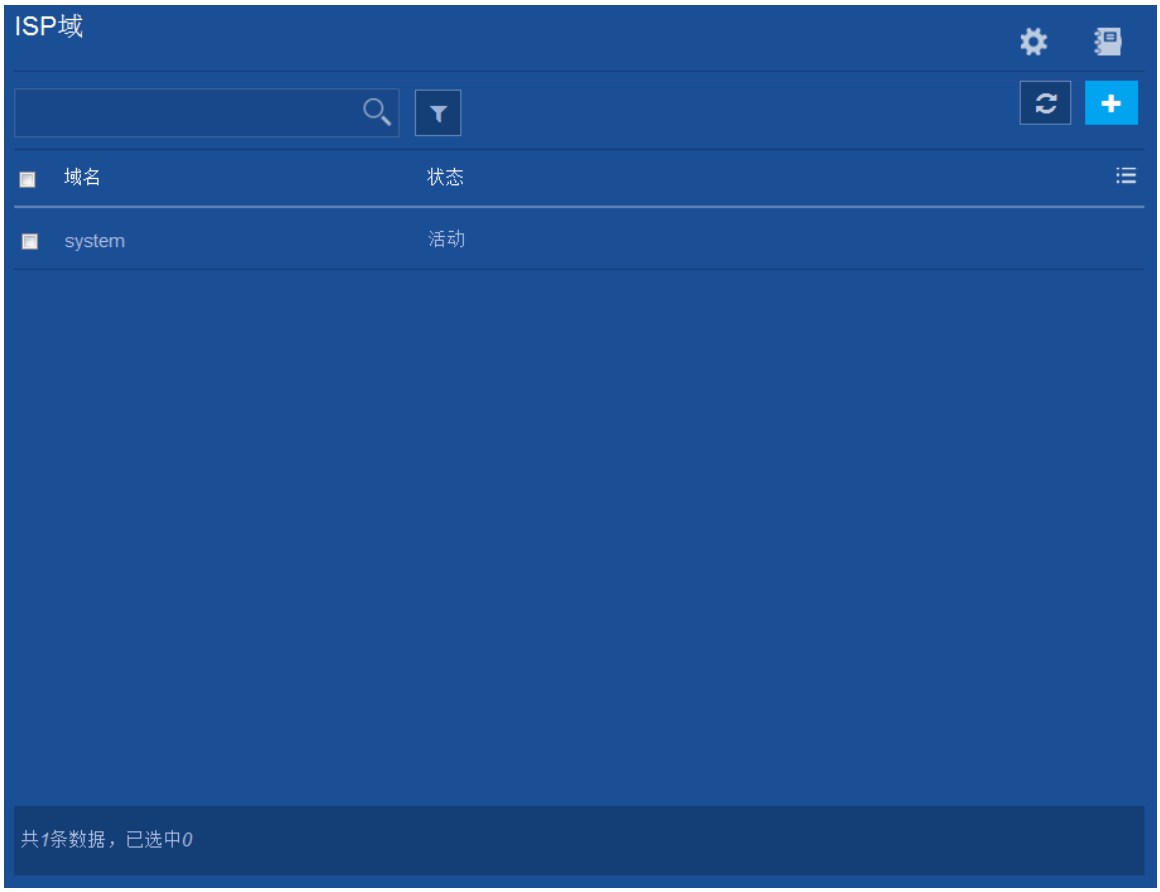
## 7.2 配置准备

- 进行本地认证时，需要配置本地用户，具体配置请参见“本地认证”。
- 进行远端认证、授权或计费时，需要配置 RADIUS 方案，通过引用已配置的 RADIUS 方案来实现认证、授权、计费。有关 RADIUS 方案的配置请参见“RADIUS”。

## 7.3 配置ISP域

(1) 在导航栏中选择“安全 > ISP 域”，进入“ISP 域”页面，如下图所示。

图7-1 ISP 域




(2) 单击可添加 ISP 域，进入“添加 ISP 域”页面，如下图所示。

图7-2 添加 ISP 域


(3) 根据需要配置参数，详细参数说明如下表所示。

(4) 单击<确定>按钮完成操作。

表7-1 添加 ISP 域的详细说明

| 标题项 | 说明 |
|---|---|
| 域名 | 设置域名 |
| 状态 | 设置 ISP 域的状态，包括活动和阻塞 |
| 接入方式 | 设置接入方式，包括登录用户、LAN接入和Portal |
| 用户闲置切断时间 | 设置用户闲置切断的时间 |
| 用户在闲置切断时间内产生的数据流量 | 设置用户在闲置切断时间内产生的数据流量 |
| 为PPP用户分配IP地址的地址池 | 设置相应地址池 |

# 8 RADIUS

## 8.1 概述

RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）是实现 AAA（Authentication, Authorization and Accounting，认证、授权和计费）的一种最常用的协议。

### 8.1.1 RADIUS 简介

RADIUS 是一种分布式的、客户端/服务器结构的信息交互协议，能保护网络不受未授权访问的干扰，常应用在既要求较高安全性、又允许远程用户访问的各种网络环境中。该协议定义了 RADIUS 的报文格式及其消息传输机制，并规定使用 UDP 作为封装 RADIUS 报文的传输层协议（UDP 端口 1812、1813 分别作为认证、计费端口）。

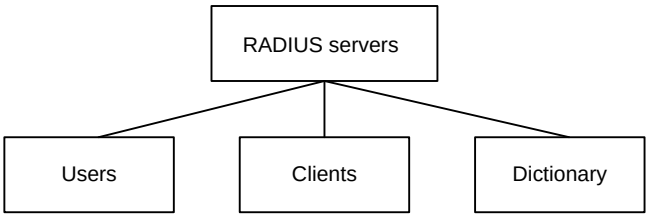
RADIUS 最初仅是针对拨号用户的 AAA 协议，后来随着用户接入方式的多样化发展，RADIUS 也适应多种用户接入方式，如以太网接入、ADSL 接入。它通过认证授权来提供接入服务，通过计费来收集、记录用户对网络资源的使用。

### 8.1.2 客户端/服务器模式

- 客户端：RADIUS 客户端一般位于 NAS 设备上，可以遍布整个网络，负责传输用户信息到指定的 RADIUS 服务器，然后根据从服务器返回的信息进行相应处理（如接受/拒绝用户接入）。
- 服务器：RADIUS 服务器一般运行在中心计算机或工作站上，维护相关的用户认证和网络服务访问信息，负责接收用户连接请求并认证用户，然后给客户端返回所有需要的信息（如接受/拒绝认证请求）。

RADIUS 服务器通常要维护三个数据库，如下图所示。

图8-1 RADIUS 服务器的组成




- “Users”：用于存储用户信息（如用户名、口令以及使用的协议、IP 地址等配置信息）。
- “Clients”：用于存储 RADIUS 客户端的信息（如接入设备的共享密钥、IP 地址等）。
- “Dictionary”：用于存储 RADIUS 协议中的属性和属性值含义的信息。

### 8.1.3 安全和认证机制

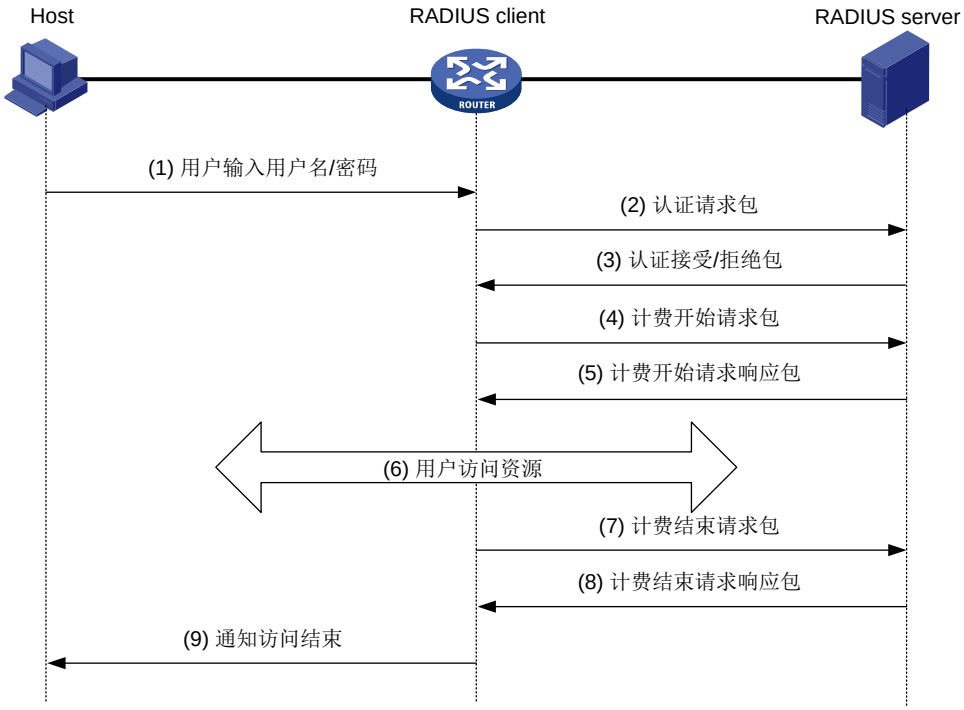
RADIUS 客户端和 RADIUS 服务器之间认证消息的交互是通过共享密钥的参与来完成的，并且共享密钥不能通过网络来传输，增强了信息交互的安全性。另外，为防止用户密码在不安全的网络上传递时被窃取，在传输过程中对密码进行了加密。

RADIUS 服务器支持多种方法来认证用户，如基于 PPP 的 PAP、CHAP 认证。另外，RADIUS 服务器还可以作为一个代理，以 RADIUS 客户端的身份与其它的 RADIUS 认证服务器进行通信，负责转发 RADIUS 认证和计费报文。

### 8.1.4 RADIUS 的基本消息交互流程

用户、RADIUS 客户端和 RADIUS 服务器之间的交互流程如下图所示。

图8-2 RADIUS 的基本消息交互流程




消息交互流程如下：

(2) 用户发起连接请求，向 RADIUS 客户端发送用户名和密码。

(3) RADIUS 客户端根据获取的用户名和密码，向 RADIUS 服务器发送认证请求包（Access-Request），其中的密码在共享密钥的参与下由 MD5 算法进行加密处理。

(4) RADIUS 服务器对用户名和密码进行认证。如果认证成功，RADIUS 服务器向 RADIUS 客户端发送认证接受包（Access-Accept）；如果认证失败，则返回认证拒绝包（Access-Reject）。由于 RADIUS 协议合并了认证和授权的过程，因此认证接受包中也包含了用户的授权信息。

(5) RADIUS 客户端根据接收到的认证结果接入/拒绝用户。如果允许用户接入，则 RADIUS 客户端向 RADIUS 服务器发送计费开始请求包（Accounting-Request）。

(6) RADIUS 服务器返回计费开始响应包（Accounting-Response），并开始计费。

(7) 用户开始访问网络资源。

(8) 用户请求断开连接，RADIUS 客户端向 RADIUS 服务器发送计费停止请求包（Accounting-Request）。

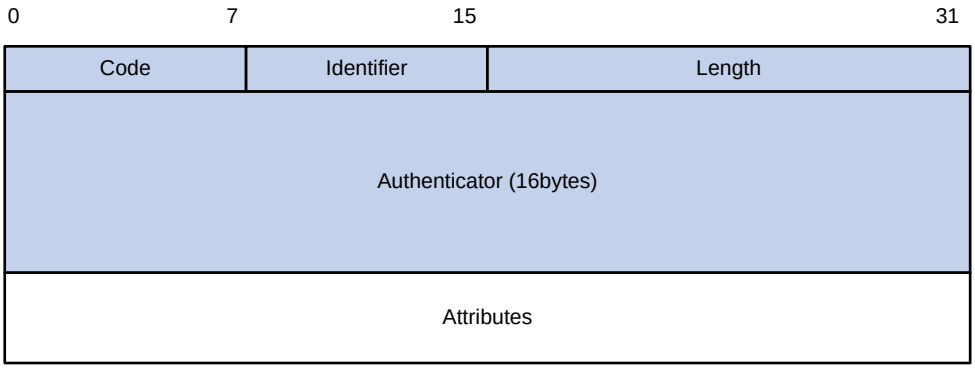
(9) RADIUS 服务器返回计费结束响应包（Accounting-Response），并停止计费。

(10) 用户结束访问网络资源。

### 8.1.5 RADIUS 报文结构

RADIUS 采用 UDP 报文来传输消息，通过定时器管理机制、重传机制、备用服务器机制，确保 RADIUS 服务器和客户端之间交互消息的正确收发。RADIUS 报文结构如下图所示。

图8-3 RADIUS 报文结构




各字段的解释如下：

(2) Code 域

长度为 1 个字节，用于说明 RADIUS 报文的类型，如下表所示。

表8-1 Code 域的主要取值说明

| Code | 报文类型 | 报文说明 |
|---|---|---|
| 1 | Access-Request认证请求包 | 方向Client->Server，Client将用户信息传输到Server，由Server判断是否接入该用户。该报文中必须包含User-Name属性，可选包含NAS-IP-Address、User-Password、NAS-Port等属性 |
| 2 | Access-Accept认证接受包 | 方向Server->Client，如果Access-Request报文中的所有Attribute值都可以接受（即认证通过），则传输该类型报文 |
| 3 | Access-Reject认证拒绝包 | 方向Server->Client，如果Access-Request报文中存在任何无法被接受的Attribute值（即认证失败），则传输该类型报文 |
| 4 | Accounting-Request计费请求包 | 方向Client->Server，Client将用户信息传输到Server，请求Server开始/停止计费，由该报文中的Acct-Status-Type属性区分计费开始请求和计费结束请求 |
| 5 | Accounting-Response计费响应包 | 方向Server->Client，Server通知Client已经收到Accounting-Request报文，并且已经正确记录计费信息 |

(3) Identifier 域

长度为 1 个字节，用于匹配请求包和响应包，以及检测在一段时间内重发的请求包。类型一致的请求包和响应包的 Identifier 值相同。

(4) Length 域

长度为 2 个字节，表示 RADIUS 数据包（包括 Code、Identifier、Length、Authenticator 和 Attribute）的长度，范围从 20～4096。超过 Length 域的字节将作为填充字符被忽略。如果接收到的包的实际长度小于 Length 域的值时，则包会被丢弃。

(5) Authenticator 域

长度为 16 个字节，用于验证 RADIUS 服务器的应答，另外还用于用户密码的加密。Authenticator 包括两种类型：Request Authenticator 和 Response Authenticator。

(6) Attribute 域

不定长度，用于携带专门的认证、授权和计费信息，提供请求和响应报文的配置细节。Attribute 可包括多个属性，每一个属性都采用（Type、Length、Value）三元组的结构来表示。

- 类型（Type），1 个字节，取值为 1～255，用于表示属性的类型，下表列出了 RADIUS 认证、授权、计费常用的属性。
- 长度（Length），表示该属性（包括类型、长度和属性）的长度，单位为字节。
- 属性值（Value），表示该属性的信息，其格式和内容由类型和长度决定，最大长度为 253 字节。

表8-2 RADIUS 属性

| 属性编号 | 属性名称 | 属性编号 | 属性名称 |
|---|---|---|---|
| 1 | User-Name | 45 | Acct-Authentic |
| 2 | User-Password | 46 | Acct-Session-Time |
| 3 | CHAP-Password | 47 | Acct-Input-Packets |
| 4 | NAS-IP-Address | 48 | Acct-Output-Packets |
| 5 | NAS-Port | 49 | Acct-Terminate-Cause |
| 6 | Service-Type | 50 | Acct-Multi-Session-Id |
| 7 | Framed-Protocol | 51 | Acct-Link-Count |
| 8 | Framed-IP-Address | 52 | Acct-Input-Gigawords |
| 9 | Framed-IP-Netmask | 53 | Acct-Output-Gigawords |
| 10 | Framed-Routing | 54 | (unassigned) |
| 11 | Filter-ID | 55 | Event-Timestamp |
| 12 | Framed-MTU | 56-59 | (unassigned) |
| 13 | Framed-Compression | 60 | CHAP-Challenge |
| 14 | Login-IP-Host | 61 | NAS-Port-Type |
| 15 | Login-Service | 62 | Port-Limit |
| 16 | Login-TCP-Port | 63 | Login-LAT-Port |
| 17 | (unassigned) | 64 | Tunnel-Type |
| 18 | Reply_Message | 65 | Tunnel-Medium-Type |
| 19 | Callback-Number | 66 | Tunnel-Client-Endpoint |
| 20 | Callback-ID | 67 | Tunnel-Server-Endpoint |
| 21 | (unassigned) | 68 | Acct-Tunnel-Connection |
| 22 | Framed-Route | 69 | Tunnel-Password |
| 23 | Framed-IPX-Network | 70 | ARAP-Password |
| 24 | State | 71 | ARAP-Features |
| 25 | Class | 72 | ARAP-Zone-Access |

| 属性编号 | 属性名称 | 属性编号 | 属性名称 |
|---|---|---|---|
| 26 | Vendor-Specific | 73 | ARAP-Security |
| 27 | Session-Timeout | 74 | ARAP-Security-Data |
| 28 | Idle-Timeout | 75 | Password-Retry |
| 29 | Termination-Action | 76 | Prompt |
| 30 | Called-Station-Id | 77 | Connect-Info |
| 31 | Calling-Station-Id | 78 | Configuration-Token |
| 32 | NAS-Identifier | 79 | EAP-Message |
| 33 | Proxy-State | 80 | Message-Authenticator |
| 34 | Login-LAT-Service | 81 | Tunnel-Private-Group-id |
| 35 | Login-LAT-Node | 82 | Tunnel-Assignment-id |
| 36 | Login-LAT-Group | 83 | Tunnel-Preference |
| 37 | Framed-AppleTalk-Link | 84 | ARAP-Challenge-Response |
| 38 | Framed-AppleTalk-Network | 85 | Acct-Interim-Interval |
| 39 | Framed-AppleTalk-Zone | 86 | Acct-Tunnel-Packets-Lost |
| 40 | Acct-Status-Type | 87 | NAS-Port-Id |
| 41 | Acct-Delay-Time | 88 | Framed-Pool |
| 42 | Acct-Input-Octets | 89 | (unassigned) |
| 43 | Acct-Output-Octets | 90 | Tunnel-Client-Auth-id |
| 44 | Acct-Session-Id | 91 | Tunnel-Server-Auth-id |

说明

上表中所列的属性由 RFC 2865、RFC 2866、RFC2867 和 RFC2568 分别定义。

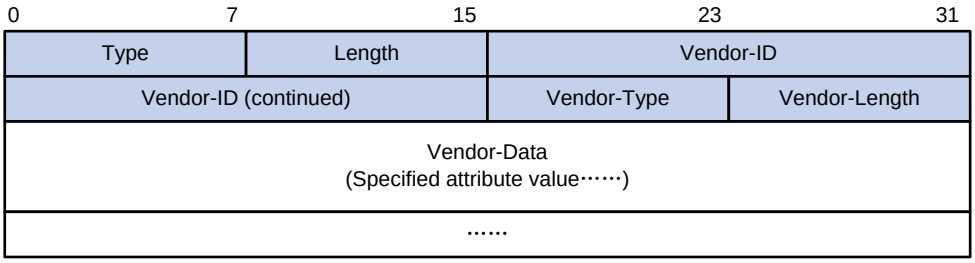
### 8.1.6 RADIUS 扩展属性

RADIUS 协议具有良好的可扩展性，协议（RFC 2865）中定义的 26 号属性（Vendor-Specific）用于设备厂商对 RADIUS 进行扩展，以实现标准 RADIUS 没有定义的功能。

设备厂商可以封装多个自定义的“（Type、Length、Value）”子属性来扩展 RADIUS。如下图所示，26 号属性报文内封装的子属性包括以下四个部分：

- Vendor-ID，表示厂商代号，最高字节为 0，其余 3 字节的编码见 RFC 1700。
- Vendor-Type，表示子属性类型。
- Vendor-Length，表示该子属性长度。
- Vendor-Data，表示该子属性的内容。

图8-4 包括扩展属性的 RADIUS 报文片断




### 8.1.7 协议规范

与 RADIUS 相关的协议规范有：

- RFC 2865：Remote Authentication Dial In User Service (RADIUS)
- RFC 2866：RADIUS Accounting
- RFC 2867：RADIUS Accounting Modifications for Tunnel Protocol Support
- RFC 2868：RADIUS Attributes for Tunnel Protocol Support
- RFC 2869：RADIUS Extensions

## 8.2 配置RADIUS方案

(1) 在导航栏中选择“安全 > RADIUS”，进入“RADIUS”页面，如下图所示。

图8-5 RADIUS


(2) 单击  ，进入添加 RADIUS 方案的配置页面，如下图所示。

图8-6 添加 RADIUS 方案


(3) 配置 RADIUS 方案，详细配置如下表所示。

(4) 单击<确定>按钮完成操作。

表8-3 RADIUS 方案的详细配置

| 配置项 | 说明 |
| --- | --- |
| 方案名称 | 设置RADIUS方案的名称 |

| 配置项 | | 说明 |
| --- | --- | --- |
| 认证服务器 | 主服务器 | 设置主服务器的信息 |
| | 备份服务器 | 设置备份服务器的信息 |
| 认证共享密钥 | | 设置认证共享密钥 |
| 计费服务器 | 主服务器 | 设置主服务器的信息 |
| | 备份服务器 | 设置备份服务器的信息 |
| 计费共享密钥 | | 设置计费共享密钥 |
| 显示高级设置 | | 单击“显示高级设置”，显示高级设置的详细信息 |
| 高级信息设置 | 发送RADIUS报文使用的源IP地址 | 设置IP地址 |
| | 发送RADIUS报文使用的源IPv6地址 | 设置IPv6地址 |
| | 服务器响应超时时间 | 设置服务器响应超时时间 |
| | 发送RADIUS报文的最大尝试次数 | 设置发送RADIUS报文的最大尝试次数 |
| | 服务器恢复活动状态的时间 | 设置服务器恢复活动状态的时间 |
| | 发送实时计费更新报文的间隔 | 设置发送实时计费更新报文的间隔 |
| | 发起实时计费更新请求的最大尝试次数 | 设置最大尝试次数 |
| | 发送给RADIUS服务器的用户名格式 | 包括与用户名输入保持一致、携带域名和不携带域名 |
| | 发送给RADIUS服务器的数据流的单位 | 包括字节、千字节、兆字节和千兆字节 |
| | 发送给RADIUS服务器的数据包的单位 | 包括包、千包、兆包和千兆包 |
| | Accounting-on | 设置是否开启Accounting-on功能 |

## 8.3 RADIUS典型配置举例

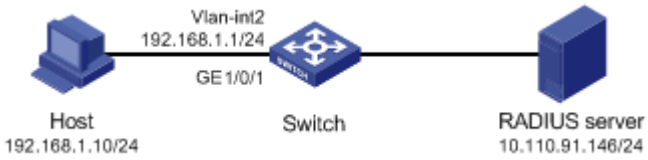
### 1. 组网需求

如下图所示，配置 Switch 实现 RADIUS 服务器对登录设备的 802.1X 用户进行认证、计费（802.1X 用户在线时长统计）。

RADIUS 服务器使用 CAMS/iMC 服务器。在 RADIUS 服务器上已经添加了 802.1X 用户的用户名和密码，同时设置了与 Switch 交互报文时的共享密钥为“expert”。

根据以上情况，只需设置 Switch 与 IP 地址为 10.110.91.146 的 RADIUS 服务器（其担当认证、计费服务器的职责，采用缺省端口进行认证和计费）进行报文交互时的共享密钥为“expert”。同时可以设置 Switch 向 RADIUS 服务器发送用户名时不带域名。

图8-7 RADIUS 配置组网图




### 2. 配置步骤

说明

开启全局和指定端口的 802.1X 特性，并配置基于 MAC 地址的接入控制方式。具体配置略。

(1) 配置各接口 IP 地址。（略）

(2) 配置 RADIUS 方案 system。

步骤 1：在导航栏中选择“安全 > RADIUS”，进入 RADIUS 的配置页面。

步骤 2：单击，进入添加 RADIUS 方案的配置页面。

步骤 3：进行如下配置，如下图所示。

- 输入方案名称为“system”。
- 在“认证服务器”的“主服务器”区域，进行如下配置：
  - 选择类型为“IP 地址”。
  - 输入 IP 地址/FQDN 为“10.110.91.146”。
  - 输入端口为“1812”。
  - 输入共享密钥为“expert”。
  - 选择状态为“活动”。
- 在“计费服务器”的“主服务器”区域，进行如下配置：
  - 选择类型为“IP 地址”。
  - 输入 IP 地址/FQDN 为“10.110.91.146”。
  - 输入端口为“1813”。
  - 输入共享密钥为“expert”。

- 选择状态为“活动”。

- 单击“显示高级设置”展开高级设置选项，设置发送给 RADIUS 服务器的用户名格式为“不携带域名”。

步骤 4：单击<确定>按钮完成操作。

图8-8 添加 RADIUS 方案 system


(3) 添加 ISP 域。

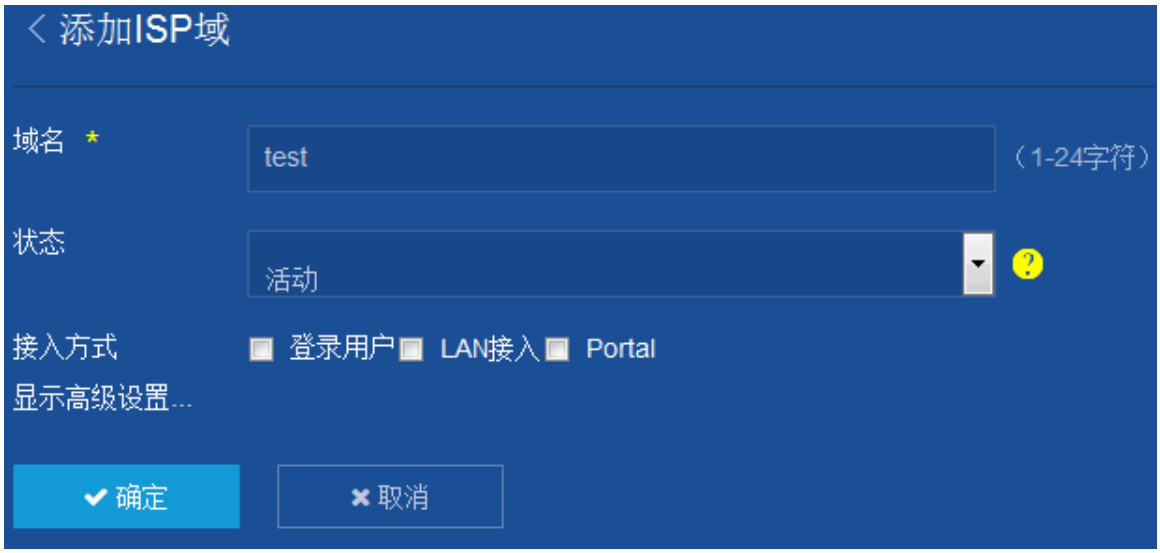
步骤 1：在导航栏中选择“安全 > ISP 域”，进入“ISP 域”页面。

步骤 2：单击  。

步骤 3：输入域名为“test”，如下图所示。

步骤 4：单击<确定>按钮完成操作。

图8-9 添加 ISP 域




## 8.4 注意事项

配置 RADIUS 客户端时需要注意如下事项：

(1) 目前 RADIUS 不支持对 FTP 用户进行计费。

(2) 如果在线用户正在使用的计费服务器被删除，则设备将无法发送用户的实时计费请求和停止计费请求，且停止计费报文不会被缓存到本地。

(3) RADIUS 方案中各服务器的状态（active、block）决定了设备向哪个服务器发送请求报文，以及设备在与当前服务器通信中断的情况下，如何转而与另外一个服务器进行交互。在实际组网环境中，可指定一个主 RADIUS 服务器和多个备份 RADIUS 服务器，由备份服务器作为主服务器的备份。通常情况下，设备上主/备份服务器的切换遵从以下原则：

- 当主服务器状态为 active 时，设备首先尝试与主服务器通信，若主服务器不可达，设备更改主服务器的状态为 block，并启动该服务器的静默定时器，然后按照备份服务器的配置先后顺序依次查找状态为 active 的备份服务器进行认证或者计费。如果状态为 active 的备份服务器也不可达，则将该备份服务器的状态置为 block，同时启动该服务器的静默定时器，并继续查找状态为 active 的备份服务器。当服务器的静默定时器超时，或者设备收到该服务器的认证/计费应答报文时，该服务器将恢复为 active 状态。在一次认证或计费过程中，如果设备在尝试与备份服务器通信时，主服务器状态由 block 恢复为 active，则设备并不会立即恢复与主服务器的通信，而是继续查找备份服务器。如果所有已配置的服务器都不可达，则认为本次认证或计费失败。

- 一个用户的计费流程开始之后，设备就不会再与其它的计费服务器通信，即该用户的实时计费报文和停止计费报文只会发往当前使用的计费服务器。如果当前使用的计费服务器被删除，则实时计费和停止计费报文都将无法发送。
- 如果在认证或计费过程中删除了服务器，则设备在与当前服务器通信超时后，将会重新从主服务器开始依次查找状态为 active 的服务器进行通信。
- 当主/备份服务器的状态均为 block 时，设备仅与主服务器通信，若主服务器可达，则主服务器状态变为 active，否则保持不变。
- 只要存在状态为 active 的服务器，设备就仅与状态为 active 的服务器通信，即使该服务器不可达，设备也不会尝试与状态为 block 的服务器通信。
- 设备收到服务器的认证或计费应答报文后会将与报文源 IP 地址相同且状态为 block 的认证或计费服务器的状态更改为 active。

(4) 实时计费间隔与用户量之间的推荐比例关系如下表所示。

**表8-4 实时计费间隔与用户量之间的推荐比例关系**

| 用户数 | 实时计费间隔（分钟） |
|---|---|
| 1～99 | 3 |
| 100～499 | 6 |
| 500～999 | 12 |
| ≥1000 | ≥15 |

# 9 TACACS

## 9.1 概述

TACACS（Terminal Access Controller Access Control System，终端访问控制器控制系统协议）安全协议基于 RFC1492，提供了增强功能。

## 9.2 配置TACACS方案

(1) 在导航栏中选择“安全 > TACACS”，进入“TACACS”页面，如下图所示。

图9-1 TACACS


(2) 单击  ，进入添加 TACACS 方案页面，如下图所示。

图9-2 添加 TACACS 方案

(3) 配置 TACACS 方案的信息，详细配置如下表所示。

(4) 单击<确定>按钮完成操作。

表9-1 TACACS 方案的详细配置

| 配置项 | | 说明 |
|---|---|---|
| 方案名称 | | 设置TACACS方案的名称 |
| 认证服务器 | 主服务器 | 设置主服务器的信息 |
| | 备份服务器 | 设置备份服务器的信息 |
| 认证共享密钥 | | 设置认证共享密钥 |
| 授权服务器 | 主服务器 | 设置主服务器的信息 |
| | 备份服务器 | 设置备份服务器的信息 |
| 授权共享密钥 | | 设置授权共享密钥 |
| 计费服务器 | 主服务器 | 设置主服务器的信息 |
| | 备份服务器 | 设置备份服务器的信息 |
| 计费共享密钥 | | 设置计费共享密钥 |
| 显示高级设置 | | 单击“显示高级设置”，显示高级设置的详细信息 |

# 10 本地认证

## 10.1 概述

本地认证模块提供了本地用户、用户组的配置功能。

### 1. 本地用户

本地用户是本地设备上设置的一组用户属性的集合。该集合以用户名为用户的唯一标识，可配置多种属性，比如用户密码、用户类型、服务类型、授权属性等。为使某个请求网络服务的用户可以通过本地认证，需要在设备上的本地用户数据库中添加相应的表项。

### 2. 用户组

用户组是一个本地用户属性的集合，某些需要集中管理的授权属性可在用户组中统一配置和管理，用户组内的所有本地用户都可以继承这些属性。

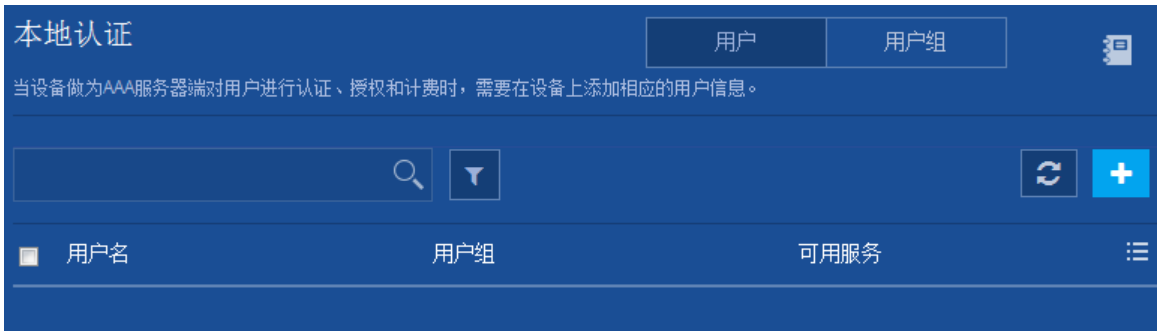
每个新增的本地用户都默认属于一个系统自动创建的用户组 system，且继承该组的所有属性，但本地用户的属性比用户组的属性优先级高。

## 10.2 配置用户

### 10.2.1 配置本地用户

(1) 在导航栏中选择“安全 > 本地认证”，默认进入“用户”页签的页面，如下图所示。

图10-1 本地用户




(2) 单击  ，进入添加用户的配置页面，如下图所示。

图10-2 添加用户


添加用户
用户名 *
（1-55字符）
密码
（1-63字符）
确认密码
用户组
请选择...
可用服务
ADVPN
IKE
LAN接入
Portal
PPP
同时在线最大用户数
(1-1024)
授权属性
• 授权ACL
（2000-5999）
• 用户闲置切断时间
分钟 （1-120）
• 授权VLAN
（1-4094）
绑定属性
• 用户接入的接口
请选择...
• 用户的IPv4地址
• 用户的MAC地址
（形如：ff-ff-ff-ff-ff-ff）
• 用户所属的VLAN
（1-4094）
确定
取消

(3) 配置用户信息，详细配置如下表所示。

(4) 单击<确定>按钮完成操作。

表10-1 用户的详细配置

| 配置项 | | 说明 |
|---|---|---|
| 用户名 | | 设置用户的名称 |
| 密码 | | 设置用户的密码和确认密码<br>用户密码和确认密码必须一致 |
| 确认密码 | | 提示<br>输入的密码如果以空格开头，则开头的空格将被忽略 |
| 用户组 | | 设置用户所属的用户组<br>用户组的配置请参见“10.2.2 配置用户组” |
| 可用服务 | | 设置用户可以使用的服务类型，包括ADVPN、IKE、LAN接入、Portal和PPP<br>提示<br>服务类型是本地认证的检测项，如果没有用户可以使用的服务类型，则该用户无法正常认证通过 |
| 同时在线最大用户数 | | 设置同时在线的最大用户数量 |
| 授权属性 | 授权ACL | 设置用户的授权ACL序号<br>提示<br>授权 ACL 只对服务类型为 PPP 和 LAN 接入的用户有效 |
| | 用户闲置切断时间 | 设置用户的有效截止时间<br>当指定了过期时间的用户进行本地认证时，接入设备检查当前系统时间是否在用户的过期时间内，若在过期时间内则允许用户登录，否则拒绝用户登录 |
| | 授权VLAN | 设置用户的授权VLAN ID<br>提示<br>授权 VLAN 只对服务类型为 LAN 接入的用户有效 |
| 绑定属性 | 用户接入的接口 | 设置用户接入的接口 |
| | 用户的IPv4地址 | 设置用户的 IPv4 地址 |
| | 用户的MAC地址 | 设置用户的 MAC 地址 |
| | 用户所属的VLAN | 设置用户所属的 VLAN |

## 10.2.2 配置用户组

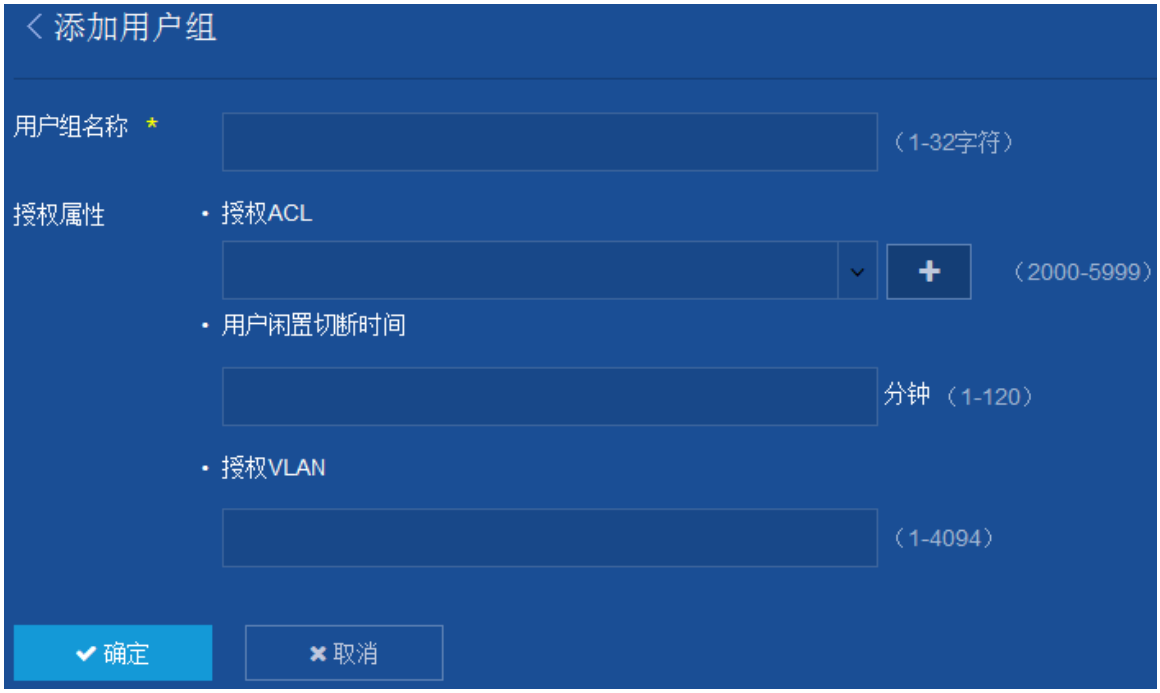
(1) 在导航栏中选择“安全 > 本地认证”。

(2) 单击“用户组”页签，进入用户组的显示页面，如下图所示。

图10-3 用户组


(3) 单击  ，进入添加用户组的配置页面，如下图所示。

图10-4 添加用户组




(4) 配置用户组，详细配置如下表所示。

(5) 单击<确定>按钮完成操作。

表10-2 用户组的详细配置

| 配置项 | 说明 |
| --- | --- |
| 用户组名称 | 设置用户组的名称 |
| 授权ACL | 设置用户组的授权ACL序号 |

| 配置项 | 说明 |
| --- | --- |
| 用户闲置切断时间 | 设置用户的有效截止时间<br>当指定了过期时间的用户进行本地认证时，接入设备检查当前系统时间是否在用户的过期时间内，若在过期时间内则允许用户登录，否则拒绝用户登录 |
| 授权VLAN | 设置用户组的授权VLAN ID |