目 录

1 802.1X

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。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。
- 仅 WX2500H-WiNet 系列不支持 slot 参数。

1.1 802.1X简介

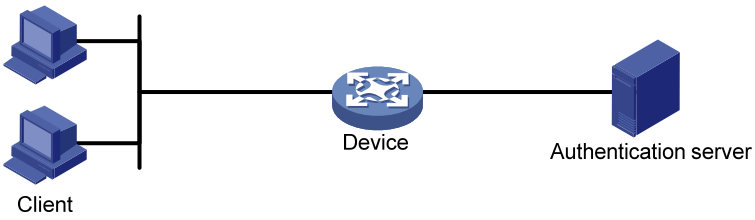
最初，提出 802.1X 协议是为解决无线局域网的网络安全问题。后来，802.1X 协议作为局域网的一种普通接入控制机制在以太网中被广泛应用，主要解决以太网内认证和安全方面的问题。

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和设备进行认证，以便控制用户设备对网络资源的访问。

1.1.1 802.1X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 图 1-1 所示。

图1-1 802.1X 体系结构图



- 客户端是请求接入局域网的用户终端，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），并通过与认证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。

1.1.2 802.1X对端口的控制

1. 受控/非受控端口

设备端为客户端提供的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。

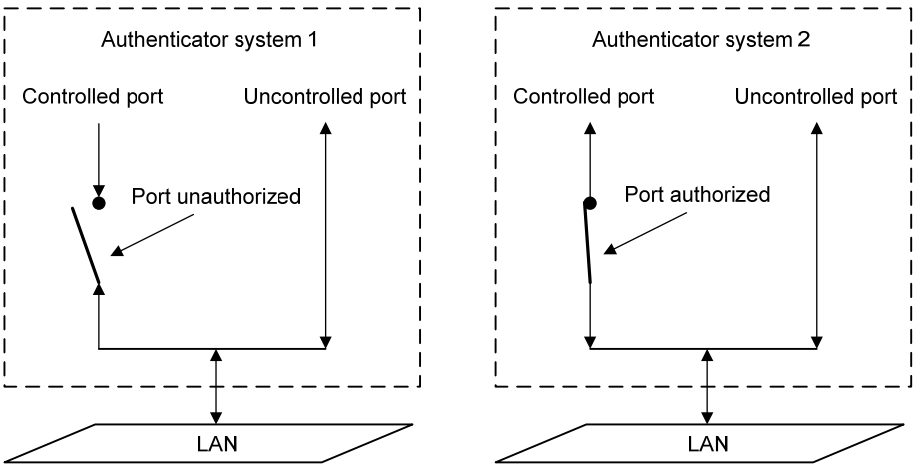
- 非受控端口始终处于双向连通状态，主要用来传递认证报文，保证客户端始终能够发出或接收认证报文。
- 受控端口在授权状态下处于双向连通状态，用于传递业务报文；在非授权状态下禁止从客户端接收任何报文。

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进行认证，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。

图 1-2 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1-2 受控端口上授权状态的影响



3. 受控方向

在非授权状态下，受控端口可以处于单向受控或双向受控状态。

- 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。

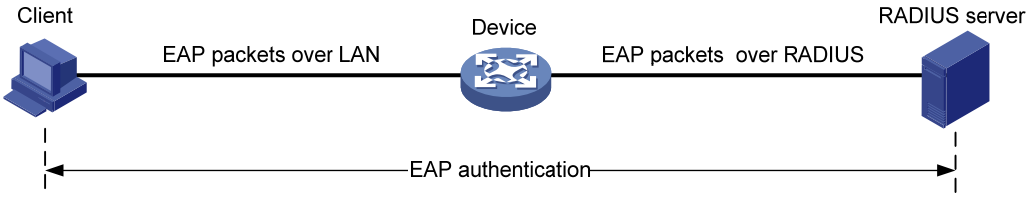
1.1.3 802.1X认证报文的交互机制

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（Extensible Authentication Protocol -Transport Layer Security，可扩展认证协议-传输层安全）、PEAP（Protected Extensible Authentication Protocol，受保护的扩展认证协议）等。在客户端与设备端之间，EAP 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 EAP 中继和 EAP 终结两种处理机制。

1. EAP中继

设备端对收到的 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。

图1-3 EAP 中继原理示意图

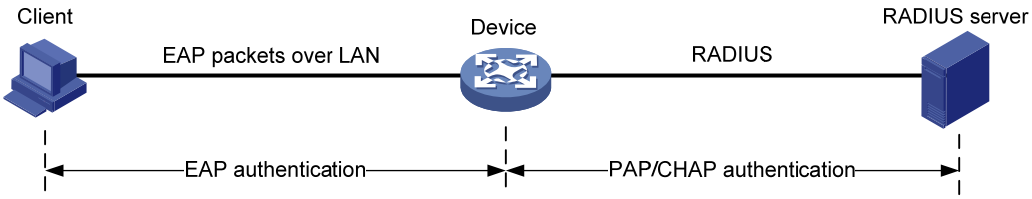


该处理机制下，EAP 认证过程在客户端和 RADIUS 服务器之间进行。RADIUS 服务器作为 EAP 服务器来处理客户端的 EAP 认证请求，设备相当于一个中继，仅对 EAP 报文做中转。因此，设备处理简单，并能够支持 EAP 的各种认证方法，但要求 RADIUS 服务器支持相应的 EAP 认证方法。

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，密码认证协议）或 CHAP（Challenge Handshake Authentication Protocol，质询握手认证协议）方法进行认证。

图1-4 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，但设备端处理较为复杂。设备端需要作为 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。

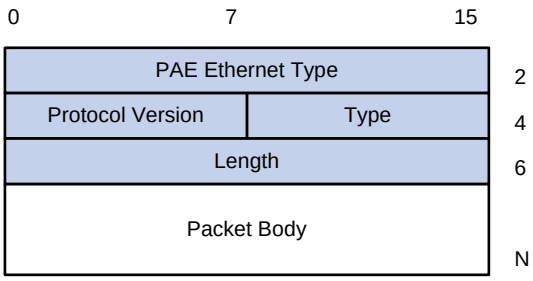
1.1.4 EAP报文的封装

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报文的封装技术，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 图 1-5 所示。

图1-5 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数据帧类型见 表 1-1。

表1-1 EAPOL 数据帧类型

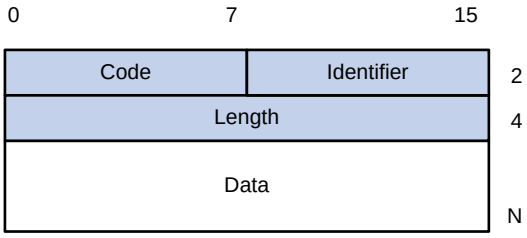
类型值	数据帧类型	说明
0x00	EAP-Packet	认证信息帧，用于承载客户端和设备端之间的EAP报文。
0x01	EAPOL-Start	认证发起帧，用于客户端向设备端发起认证请求
0x02	EAPOL-Logoff	退出请求帧，用于客户端向设备端发起下线请求

- 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 图 1-6 所示。

图1-6 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。

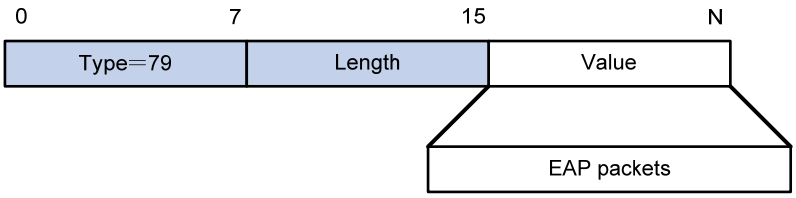
2. EAP报文在RADIUS中的封装

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“安全配置指导”中的“AAA”的 RADIUS 协议简介部分。

(1) EAP-Message

如 图 1-7 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。

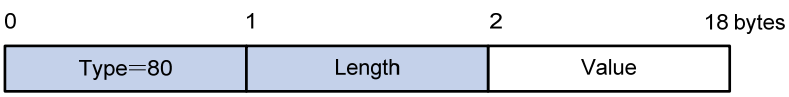
图1-7 EAP-Message 属性封装



(2) Message-Authenticator

如 图 1-8 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1-8 Message-Authenticator 属性封装



1.1.5 802.1X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，而造成设备端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：设备每隔一定时间（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。

1.1.6 802.1X的认证过程

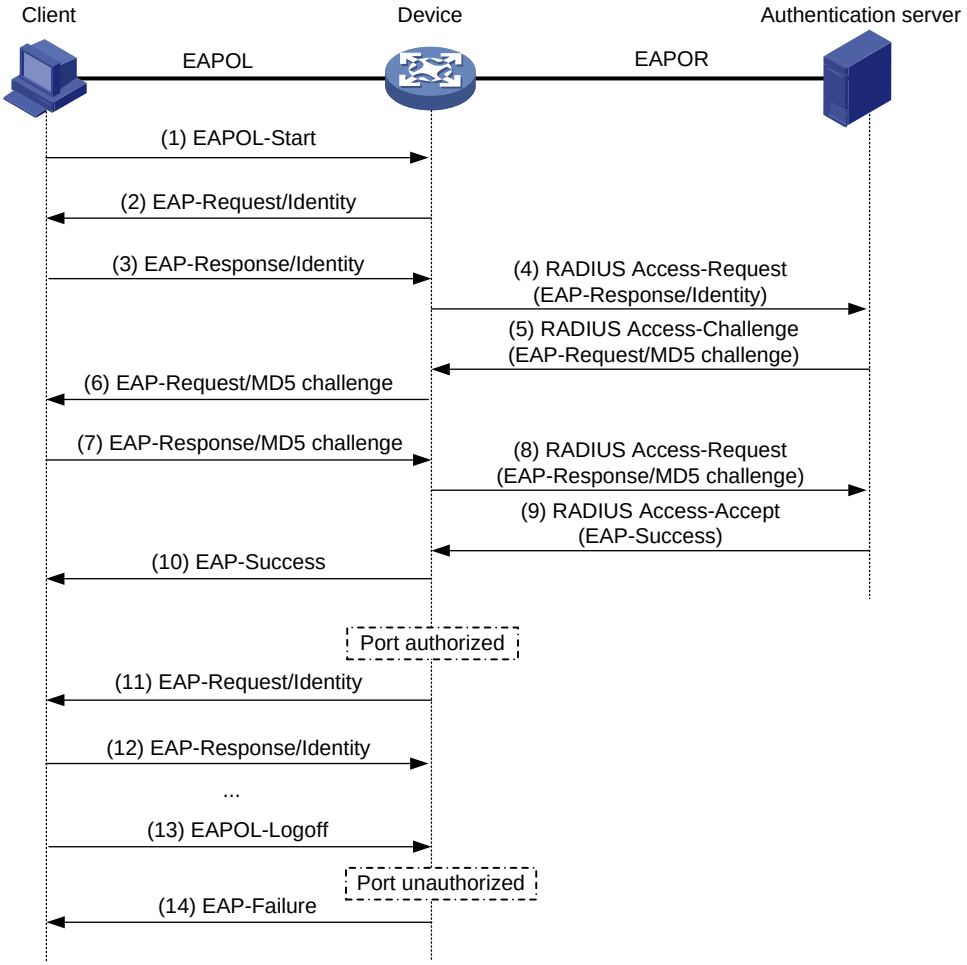
设备端支持采用 EAP 中继方式或 EAP 终结方式与远端 RADIUS 服务器交互。以下关于 802.1X 认证过程的描述，都以客户端主动发起认证为例。

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 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 1-9 所示，以MD5-Challenge类型的EAP认证为例，具体认证过程如下。

图1-9 IEEE 802.1X 认证系统的 EAP 中继方式认证流程



(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端发出认证请求帧（EAPOL-Start），开始启动一次认证过程。

(2) 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。

(3) 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。

(4) 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。

(5) 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。

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

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

(8) 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 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，并向设备端发送认证通过报文（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），并将端口改为授权状态，允许用户通过端口访问网络。

(11) 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。

(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。

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

(14) 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。

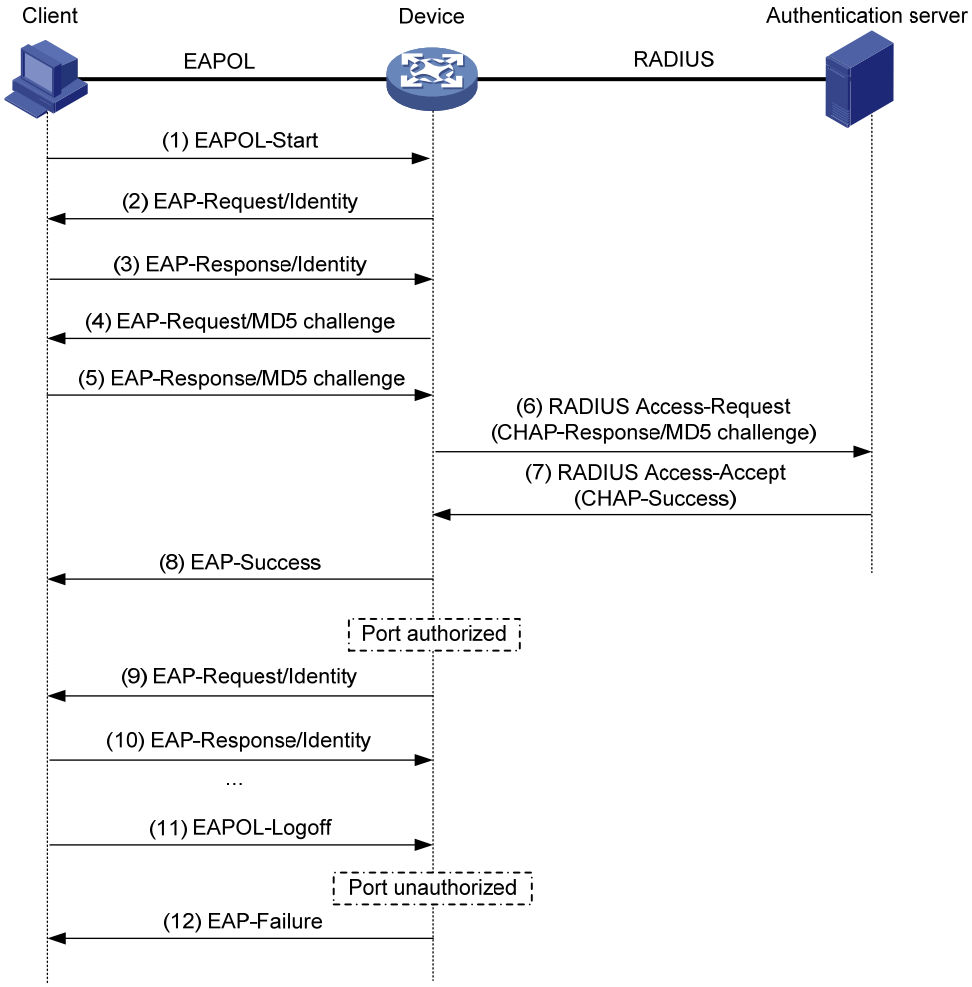
说明

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，只需要通过 **dot1x authentication-method eap** 命令启动 EAP 中继方式即可。

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。如 图 1-10 所示，以CHAP认证为例，具体的认证流程如下。

图1-10 IEEE 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发送给 RADIUS 服务器，进行相关的认证处理。

1.2 802.1X支持VLAN下发

802.1X 支持 VLAN 下发的相关内容请参考“WLAN 配置指导”中的“WLAN 用户接入认证”。

1.3 802.1X支持ACL下发

802.1X 支持 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 对用户所在端口的数据流进行过滤。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。

1.4 802.1X支持User Profile下发

802.1X 支持 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。

1.5 802.1X支持EAD快速部署

EAD（Endpoint Admission Defense，端点准入防御）作为一个网络端点接入控制方案，它通过安全客户端、安全策略服务器、接入设备以及第三方服务器的联动，加强了对用户的集中管理，提升了网络的整体防御能力。但是在实际的应用过程中 EAD 客户端的部署工作量很大，例如，需要网络管理员手动为每一个 EAD 客户端下载、升级客户端软件，这在 EAD 客户端数目较多的情况下给管理员带来了操作上的不便。

802.1X 认证支持的 EAD 快速部署功能就可以解决以上问题，它允许未通过认证的 802.1X 用户访问一个指定的 IP 地址段（称为 Free IP），并可以将用户发起的 HTTP 访问请求重定向到该 IP 地址段中的一个指定的 URL，实现用户自动下载并安装 EAD 客户端的目的。

1.6 802.1X配置任务简介

表1-2 802.1X 配置任务简介

配置任务	说明	详细配置
配置802.1X系统的认证方法	必选	1.7.2
配置设备向接入用户发送认证请求报文的最大次数	可选	1.7.3
配置802.1X认证超时定时器	可选	1.7.4
配置802.1X支持的域名分隔符	可选	1.7.5
配置802.1X支持EAD快速部署	可选	1.8

1.7 配置802.1X

1.7.1 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 认证域及其使用的 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**。

1.7.2 配置 802.1X系统的认证方法

设备上的 802.1X 系统采用的认证方法与设备对于 EAP 报文的处理机制有关，具体如下：

- 若指定 **authentication-method** 为 **eap**，则表示设备采用 EAP 中继认证方式。该方式下，设备端对客户端发送的 EAP 报文进行中继处理，并能支持客户端与 RADIUS 服务器之间所有类型的 EAP 认证方法。
- 若指定 **authentication-method** 为 **chap** 或 **pap**，则表示设备采用 EAP 终结认证方式，该方式下，设备端对客户端发送的 EAP 报文进行本地终结，并能支持与 RADIUS 服务器之间采用 CHAP 或 PAP 类型的认证方法。

表1-3 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

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”。

1.7.3 配置设备向接入用户发送认证请求报文的最大次数

如果设备向用户发送认证请求报文后，在规定的时间里（可通过命令 **dot1x timer tx-period** 或者 **dot1x timer supp-timeout** 设定）没有收到用户的响应，则设备将向用户重发该认证请求报文，若设备累计发送认证请求报文的次数达到配置的最大值后，仍然没有得到用户响应，则停止发送认证请求。

表1-4 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** *retries*	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

1.7.4 配置 802.1X认证超时定时器

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两种：

- 客户端认证超时定时器：当设备端向客户端发送了 EAP-Request/MD5 Challenge 请求报文后，设备端启动此定时器，若在该定时器设置的时长内，设备端没有收到客户端的响应，设备端将重发该报文。
- 认证服务器超时定时器：当设备端向认证服务器发送了 RADIUS Access-Request 请求报文后，设备端启动该定时器，若在该定时器设置的时长内，设备端没有收到认证服务器的响应，设备端将重发认证请求报文。

一般情况下，无需改变认证超时定时器的值，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1-5 配置 802.1X 认证超时定时器

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
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

1.7.5 配置 802.1X支持的域名分隔符

每个接入用户都属于一个 ISP 域，该域是由用户登录时提供的用户名决定的，若用户名中携带域名，则设备使用该域中的 AAA 配置对用户进行认证、授权和计费，否则使用系统中的缺省域；若设备指定了 802.1X 的强制认证域，则无论用户名中是否携带域名，设备均使用指定的强制认证域。因此，设备能够准确解析用户名中的纯用户名和域名对于为用户提供认证服务非常重要。由于不同的 802.1X 客户端所支持的用户名域名分隔符不同，为了更好地管理和控制不同用户名格式的 802.1X 用户接入，需要在设备上指定 802.1X 可支持的域名分隔符。

目前，802.1X 支持的域名分隔符包括 @、\、.、和 /，对应的用户名格式分别为 *username@domain-name*，*domain-name\username*，*username.domain-name* 和 *username/domain-name*，其中 *username* 为纯用户名、*domain-name* 为域名。如果用户名中包含有多个域名分隔符字符，则设备仅将最后一个出现的域名分隔符识别为实际使用的域名分隔符，例如，用户输入的用户名为 123/22\@abc，设备上指定 802.1X 支持的域名分隔符为/、\，则识别出的纯用户名为@abc，域名为 123/22。

需要注意的是：

- 如果用户输入的用户名中不包含任何 802.1X 可支持的域名分隔符，则设备会认为该用户名并未携带域名，则使用系统中的缺省域对该用户进行认证。
- 若设备上指定发送给认证服务器的用户名携带域名（**user-name-format with-domain**），则发送给认证服务器的用户名包括三个部分：识别出的纯用户名、域名分隔符@、最终使用的认证域名。例如，用户输入的用户名为 121.123/22\@abc，指定 802.1X 支持的域名分隔符为 /、\、.，最终使用的认证域为 xyz，则发送给认证服务器的用户名为@abc@xyz。

  user-name-format 命令的具体介绍请参考“安全命令参考”中的“AAA”。

- 为保证用户信息可在认证服务器上被准确匹配到，设备上指定的 802.1X 支持的域名分隔符必须与认证服务器支持的域名分隔符保持一致，否则可能会因为服务器匹配用户失败而导致用户认证失败。

表1-6 指定 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@

1.8 配置802.1X支持EAD快速部署


说明

目前，MAC 地址认证和端口安全特性不支持 EAD 的快速部署功能，全局使能 MAC 认证或端口安全功能将会使 EAD 快速部署功能失效。

1.8.1 配置Free IP

全局使能 EAD 快速部署功能且配置 Free IP 之后，未通过认证的 802.1X 终端用户可以访问该 IP 地址段中的网络资源。该 IP 地址段中可以配置一个或多个特定服务器，用于提供 EAD 客户端的下载升级或者动态地址分配等服务。

需要注意的是：

- MAC 地址认证、端口安全功能均与 Free IP 配置互斥。
- 未通过 802.1X 认证的用户若要通过外网的 DHCP 服务器动态获得 IP 地址，则需要保证该 DHCP 服务器的 IP 地址在配置的 Free IP 内。

表1-7 配置 Free IP

配置步骤	命令	说明
进入系统视图	**system-view**	-
全局使能EAD快速部署功能	**dot1x ead-assistant enable**	缺省情况下，未使能EAD快速部署功能
配置Free IP	**dot1x ead-assistant free-ip** *ip-address* { *mask-length* | *mask-address* }	缺省情况下，未定义Free IP

1.8.2 配置用户HTTP访问的重定向URL

802.1X 终端用户在认证成功之前，如果使用浏览器访问网络，设备会将用户访问的 URL 重定向到已配置的 URL（例如，重定向到 EAD 客户端下载界面），这样只要用户打开浏览器，就必须进入管理员预设的界面。重定向的 URL 必须处于 Free IP 网段内，否则无法实现重定向。

表1-8 配置用户 HTTP 访问的重定向 URL

配置步骤	命令	说明
进入系统视图	**system-view**	-
配置用户HTTP访问的重定向URL	**dot1x ead-assistant url** *url-string*	缺省情况下，未定义重定向URL

1.8.3 配置EAD规则的老化时间

EAD 快速部署功能通过制订 EAD 规则（通常为 ACL 规则）来给予未通过认证的终端用户受限制的网络访问权限，在用户认证成功后，所占用的 ACL 将被释放。由于设备支持的 ACL 数量有限，当大量用户同时认证时，ACL 资源将迅速被占用，如果没有用户认证成功，将出现 ACL 数量不足的情况，这样会导致一部分新接入的用户无法认证。

管理员可以通过配置 EAD 规则的老化时间来控制用户对 ACL 资源的占用，当用户访问网络时该定时器即开始计时，在定时器超时或者用户下载客户端并成功通过认证之后，该用户所占用的 ACL 资源即被删除，这样那些在老化时间内未进行任何操作的用户所占用的 ACL 资源会及时得到释放。在接入用户数量较多时，可以将超时时间适当缩短，以提高 ACL 的使用效率。

表1-9 配置 EAD 规则老化时间

配置步骤	命令	说明
进入系统视图	**system-view**	-
配置EAD规则老化时间	**dot1x timer ead-timeout** *ead-timeout-value*	缺省情况下，EAD规则老化时间为30分钟

1.9 802.1X显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 802.1X 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 802.1X 的统计信息。

表1-10 802.1X 显示和维护

操作	命令
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**] [**ap** *ap-name* [**radio** *radio-id*]]
显示当前802.1X在线用户的详细信息	**display dot1x connection** [**ap** *ap-name* [**radio** *radio-id*] | **slot** *slot-number* | **user-mac** *mac-addr* | **user-name** *name-string*]
清除802.1X的统计信息	**reset dot1x statistics** [**ap** *ap-name* [**radio** *radio-id*]]

1.10 常见配置错误举例

1.10.1 用户通过浏览器访问外部网络不能正确重定向

1. 故障现象

用户在浏览器中输入地址，但该 HTTP 访问不能被正确重定向到指定的 URL 服务器。

2. 故障分析

- 用户在浏览器地址栏内输入了字符串类型的地址。由于用户主机使用的操作系统首先会将这个字符串地址作为名字进行网络地址解析，如果解析不成功通常会以非 X.X.X.X 形式的网络地址发送 ARP 请求，这样的请求不能进行重定向；
- 用户在 IE 地址栏内输入了 Free IP 内的任意地址。设备会认为用户试图访问 Free IP 内的某台主机，而不对其进行重定向，即使这台主机不存在；
- 用户在配置和组网时没有将服务器加入 Free IP，或者配置的 URL 为不存在的地址，或者该 URL 指向的服务器没有提供 Web 服务。

3. 处理过程

- 地址栏内输入的地址应该为 X.X.X.X（点分十进制格式）的非 Free IP 地址才有效。
- 确保设备及服务器上的配置正确且有效。